НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки

Кафедра технічної кібернетики

«На правах рукопису»
УДК 004.045

«До захисту допущено»
Завідувач кафедри
_____ І.Р. Пархомей
(підпис)
“___”_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 126 «Інформаційні системи та технології»

на тему: Система сертифікації даних на основі блокчейн технології

Виконав: студент другого курсу, групи ІК-71мп
(шифр групи)
Осін Олександр Дмитрович _____
(прізвище, ім’я, по батькові) (підпис)

Науковий керівник доцент, к.т.н., доцент Бурлаков В. М.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2018 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Факультет інформатики та обчислювальної техніки
Кафедра технічної кібернетики

Рівень вищої освіти – другий (магістерський)

Спеціальність 126 «Інформаційні системи та технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ І.Р. Пархомей
(підпис)
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Осіну Олександру Дмитровичу
(прізвище, ім'я, по батькові)

1. Тема дисертації «Система сертифікації даних на основі блокчейн технології»,

науковий керівник дисертації доцент, к.т.н., доцент Бурлаков В. М.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «__07_»___11____ 2018 р. № 4112-с

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження – система сертифікації даних на основі блокчейн технології.

4. Предмет дослідження – процес сертифікації, підтвердження наукових досягнень та інших цифрових даних.

5. Перелік завдань, які потрібно розробити – аналіз проблеми та існуючих рішень; аналіз і реалізація процесу сертифікації даних, створення цифрового підпису, розробка системи сертифікації даних за допомогою блокчейн технології та цифрового підпису; дослідження ефективності, надійності та криптостійкості розробленого програмного забезпечення.

6. Орієнтовний перелік ілюстративного матеріалу – шість плакатів

7. Орієнтовний перелік публікацій – дві публікації

8. Консультанти розділів дисертації

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Аналіз предметної області	13.09.2018 р.	
2	Постановка задачі	15.09.2018 р.	
3	Аналіз інформаційного забезпечення	20.09.2018 р.	
5	Аналіз алгоритмічного забезпечення	25.09.2018 р.	
6	Розробка алгоритмічного забезпечення	15.10.2018 р.	
7	Розробка програмного забезпечення	01.11.2018 р.	
8	Маркетинговий аналіз стартап-проекту	10.11.2018 р.	
9	Висновки	15.11.2018 р.	

Студент _____ Осін О. Д.
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ Бурлаков В. М.
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

Магістерська дисертація на тему «Система сертифікації даних на основі блокчейн технології» містить 81 сторінки, 16 ілюстрацій, 16 таблиць, 5 креслення і 13 бібліографічних найменувань за переліком посилань.

Головною метою магістерської дисертації є підвищення надійності системи сертифікації, довіри до процесу сертифікації, перевірки валідності сертифікованих даних за допомогою блокчейн технології та зберігання і обмін конфеденційними даними без централізованої системи.

В процесі виконання проекту було проведено дослідження предметної області, а саме існуючих систем сертифікації, їх функціонал та можливості, на основі яких були сформовані вимоги до розроблюваної системи. Спроектовано прототип архітектури системи з основними компонентами. Реалізовано процес розгортання системи та написано документацію до проекту.

Перелік ключових слів: блокчейн, сертифікація, емітент, біткойн, ethereum, криптовалюта, транзакція, акредитація, цифровий підпис, REST архітектура, API.

ABSTRACT

Master's thesis: "Blockchain-based data certification system" contains 81 pages, 16 illustrations, 16 tables, 5 drawing application and 13 bibliographic titles for references.

The main purpose of the master's thesis is to increase the reliability of the certification system, trust in the certification process, verify the validity of certified data based on blockchain technology and the storage and exchange of confidential data without a centralized system.

In the course of the project implementation, a field study was conducted, namely existing certification systems, their functionality and capabilities, on the basis of which the requirements for the developed system were formed. A prototype of the architecture of the system with the main components was designed. The process of deployment of the system has been implemented and the documentation for the project has been written.

The key words: blockchain, certification, issuer, bitcoin, ethereum, cryptocurrency, transaction, accreditation, digital signature, REST architecture, API.

Пояснювальна записка
до магістерської дисертації

на тему: Система сертифікації даних на основі блокчейн технології

Київ - 2018 року

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ECTS - European Credit Transfer and Accumulation System

EQAR - European Quality Assurance Register

MIT - Massachusetts Institute of Technology

SHA-256 - Secure Hash Algorithm Version 2

API - application programming interface

JSON - JavaScript Object Notation

QR-код - Quick Response Code

WSGI - Web Server Gateway Interface

БД – база даних

DRF – Django Rest Framework

ВСТУП

Інноваційна технологія блокчейн має унікальні можливості функціонування практично в будь-якій сфері життєдіяльності суспільства. Децентралізовані платформи швидко показали користувачам мережі, що вони допомагають економити час і фінансові ресурси, домагаючись кращих результатів в порівнянні з традиційними підходами.

Актуальність теми дослідження. Захист від підроблення академічних сертифікатів є давньою проблемою в академічній спільноті. Більшість сертифікатів все ще видаються на паперовому або іншому фізичному форматі. Багато країн використовують гібридні сертифікати, за допомогою яких паперові сертифікати підтримуються цифровими базами даних. Система сертифікації потребує розробки нових методів видачі, сертифікування та підтвердження різних цифрових даних, які потрібно зберігати та передавати між різними сторонами. Проте суттєві обмеження кожної системи явно свідчать про необхідність кращої, більш надійної технології сертифікації. Нова система потребує високої надійності і довіри користувачів, зацікавлених в сертифікації та підтвердженні валідності даних.

Мета і задачі дослідження.

Проектування системи сертифікації даних за допомогою блокчейн технології, яка дозволить підвищити надійність системи, довіру до процесу сертифікації та перевірки валідності даних. Також система має вдосконалювати процес зберіганння та обмін конфедеційними даними без централізованої керуючої системи.

Об'єкт дослідження. Система сертифікації даних за допомогою блокчейн технології.

Предмет дослідження. Процес та методи сертифікації, алгоритми підпису та підтвердження сертифікованих цифрових даних.

Практичне значення результатів. Розроблена система може застосовуватися для вдосконалення та підвищення надійності процесу сертифікації, верифікації та зберігання цифрових даних, таких як сертифікати навчальних досягнень. Така система можлива для застосування різними зацікавленими сторонами: студенти, науковці, навчальні установи, корпорації, установи пошуку робітників з відповідними навичками.

Структура роботи. Дипломний проект складається з 4 розділів. В першому розділі розробляються вимоги до системи на основі існуючих систем. У наступному розділі описується процес проектування та розробки системи, представляються архітектурні рішення, інструментальні засоби та основні модулі розроблюваної системи. Після етапу розробки приводиться опис розгортання додатку та створення документації по проекту. В останньому розділі розглядаються питання розробки стартап проекту та бізнес моделі.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ СУЧАСНИХ МЕТОДІВ ТА ПРОЦЕСІВ СЕРТИФІКАЦІЇ ДАНИХ

1.1 Основні поняття сертифікації

Загалом, сертифікація описує будь-який процес, за яким видається сертифікат, як перевірка справжності інформації. У освіті сертифікація використовується у багатьох випадках, наприклад, сертифікація:

- свідчення досягнення результатів навчання учнем незалежно від форми та ступеня навчання;
- освітньої організації або курсу, що відповідає певним критеріям якості;
- компетенції вчителя;
- навчального процесу відповідного курсу або предмету;
- матеріалів по яким здійснюється навчання;
- органу акредитації, який уповноважений видавати сертифікати.

Застарілі системи обліку введення сертифікації обмежують створення нових способів отримання освіти, зокрема для тих, хто не має можливості, доступу до навчальних закладів та найбільше потребує розроблення нової системи акредитації освітніх досягнень. Головним завданням для людей, які не мають формальної освіти, - це використовувати здобуті навички під час навчання на роботі, а оскільки вони часто не мають документів, що підтверджують їх навички та досвід, вони не можуть працювати на певній посаді, отримувати підвищення тощо. Більше того, існуючі системи обліку значною мірою сприяють формальній освіті за іншим навчальним досвідом, що ускладнює розробку цінних програм післядипломної освіти та післядипломної освіти - це, незважаючи на чіткі переваги навчання протягом усього життя та неформальної освіти за допомогою інтернету. Сертифікати допомагають нам визначити людей, які мають певні навички та досвід для певної роботи. Тому глобальна система сертифікації дозволить визначати рівень освіченості населення цілого міста, країни чи навіть у всьому світі.

Сертифікація в її загальній формі є питанням заяви від однієї сторони до іншої про те, що певний набір фактів є істинним. Таким чином, будь-яка сертифікація включає наступні елементи:

1. Заявка - твердження, що "цей набір фактів є істинним". Приклади навчального контексту можуть включати: "учень отримав навички", "вчитель має достатні знання для навчання" або "студент закінчив завдання, курс".

2. Емітент - орган, який перевірив та підтвердив факти, і підтверджує, що заявка є правдивою.

3. Докази, що підтверджують претензію, як правило, включають процедуру перевірки позову та певну додаткову інформацію про заявку. Таким чином, наприклад, якщо установа засвідчує, що студент отримав ECTS сертифікат, керівництво ECTS описує, як компоненти так і порядок перевірки цієї претензії. У цьому прикладі процедура передбачає тестування студента на досягнення певного набору результатів навчання, які були досягнуті через за певний проміжок часу навчання.

4. Одержувач - особа, яка розглядається заявкою - освітяни, що набувають вміння, вчитель, який має достатньо знань для навчання, або студент, який виконав завдання.

5. Сертифікат - це документ, що підтверджує особу емітента, ідентичність одержувача, заявку та наводить докази, якщо це необхідно.

6. Сертифікат включатиме підпис, який є унікальним символом, печаткою, зображенням або кодом, який може бути тільки прикріплений емітентом, і тим самим підтверджують їхню особу, установу чи іншу акредаційну систему.

1.2 Процеси сертифікації

Сертифікація передбачає три різні процеси:

1. Емісія - це процес реєстрації заяви, претензії, емітента, доказів, одержувача та підпису на сертифікат. Часто ці дані фіксуються або в

централізованій базі даних обліку заявок, або на сертифікаті, виданому одержувачу.

2. Верифікація - це процес, за допомогою якого сторона перевіряє справжність сертифіката. Існує три способи верифікації: а) перевірка, використовуючи функції безпеки, вбудовані в сам сертифікат, які можуть включати такі заходи, як перевірка автентичності печатки, спеціального паперу, підпису тощо; б) перевірка сертифіката оригінальному емітенту, за допомогою якої сторона контактує з оригінальним емітентом, запитуючи, чи дійсно він видав сертифікат, шляхом перевірки через свою централізовану базу даних або функцій безпеки, вбудованих в сертифікат; в) перевірка за допомогою централізованої бази даних заявок та сертифікатів, такі бази даних можуть бути приватними чи публічними. У випадку публічної бази даних, будь-який користувач може ознайомитися з цією базою даних, щоб переглянути цифрові копії всіх випущених сертифікатів, зробити пошук відповідного сертифікату та підтвердити тим самим дійсність виданих сертифікатів.

3. Обмін - це процес, за допомогою якого одержувач сертифіката ділиться цим сертифікатом із сторонніми особами. Є три способи спільного використання сертифікатів: а) безпосередня передача сертифікату (або копії сертифіката) сторонній особі, наприклад, по електронній пошті або шляхом індивідуального представлення стороннім особам; б) зберігання сертифікату за допомогою іншої особи, приватної бази даних, до якої надається доступ тільки з вашого дозволу і певним особам (наприклад, у разі приватної волі нотаріус має право лише поділитися вмістом заповіту з бенефіціарами); в) оприлюднення сертифікату шляхом розміщення його в публічному реєстрі або базі даних, де кожен користувач мережі може переглядати видані сертифікати.

1.3 Вимоги до системи сертифікації

Хоча будь-яка особа може видавати сертифікат будь-якій іншій особі, що підтверджує що-небудь, метою системи сертифікації є сертифікати, які широко

приймаються третіми сторонами. Це вимагає від третіх сторін значної довіри до системи та її процесів. Довіра в контексті сертифікації створюється за допомогою різних методів та процесів. Метод ідентифікації-підтвердження - цей метод передбачає створення довіри шляхом перевірки того, хто бере участь у транзакції. Оскільки сертифікат передбачає випуск заяви від однієї сторони до іншої, важливо мати можливість перевірки ідентичності як емітента, так і власника сертифіката. Ідентифікацію зазвичай перевіряють, використовуючи ідентифікаційні документи, які самі є сертифікатами, що засвідчують особу. Зазвичай третя сторона бере участь у перевірці ідентичності будь-якої із сторін. Але перевірка документів, що посвідчують особу, може бути надто складною та займати багато часу.

У деяких випадках третя сторона може захотіти отримати інформацію про те, як видаються сертифікати, зокрема, показавши методологію, яку використовує емітент під час видачі сертифікатів. Емітенту необхідно забезпечити, щоб всі сертифікати в рамках системи випускалися передбачувано і справедливо, це означає, що сертифікат буде виданий будь-якій особі, коли вона відповідає певним набором критеріїв, і тільки тоді, коли вона відповідає набору критеріїв. Це вимагає, щоб методологія була задокументована у стандарті, який дотримуються всі емітенти. Якщо система сертифікації має кілька емітентів, і кожен емітент застосовує індивідуальні або фірмові стандарти для видачі сертифікатів, неминучим результатом є створення кількох підсистем. Це, у свою чергу, повинно бути індивідуально та незалежно зрозумілим і підтвердженим для створення довіри. Тому в системі з кількома емітентами, чим вище рівень стандартизації по всій мережі, тим вище буде рівень довіри, властивий цій системі сертифікації.

Створивши стандартизовану систему сертифікатів, треба ще довіряти, що кожна сторона в системі діє сумлінно і застосовує ці стандарти відповідно до їхніх вимог. Таким чином, система сертифікації повинна включати в себе

механізм перевірки того, що сторони діють сумлінно, і виявити (і, можливо, видалити) сторони, які цього не роблять. Такий механізм призводить до більш високого рівня довіри до всієї системи.

Третя сторона, яка бажає перевірити справжність претензії в сертифікаті, повинна мати можливість гарантувати, що такий сертифікат не підроблений. Існує два способи запобігання таким підробкам:

- за допомогою фізичних механізмів боротьби з підробками, таких як підписи, водяні знаки, спеціальні конструкції, включені в сам сертифікат, що гарантує, що тільки емітент міг би скласти такий спеціальний сертифікат;
- через базу даних випущених сертифікатів, що зберігаються як емітентом, так і в централізованій базі даних, відомій як реєстр, за допомогою чого сторона може перевірити справжність сертифікату.

Ще одним елементом для довіри до сертифіката є доступність. Це означає, що одержувач сертифіката повинен мати можливість зберігати копію свідоцтва, також треті сторони, які потребують доступу до сертифікату, можуть легко отримати його власником, емітентом або реєстром. Сертифікат повинен містити інформацію про те, як перевірити претензію, а також стандарти та процеси, що використовуються для подання заяви та видачі сертифіката.

Інформація в сертифікаті повинна бути чіткою, зрозумілою та зручною у використанні. Способи здійснення цього включають стандартизацію вмісту самого сертифікату та забезпечення сертифіката цифровою копією.

1.4 Застосування сертифікації в освіті

Сертифікати широко застосовуються в різних галузях освіти. Сертифікати, як правило, видаються учням для розпізнавання:

- завершення конкретного навчання. Приклади цього можуть включати сертифікат про закінчення навчання за спеціальністю, свідоцтво про участь / участь у неформальній освіті або сертифікат, що підтверджує певний досвід;

- сукупність навчання, досягнутого у конкретній сфері, наприклад, сертифікат, що підтверджує отримання певного ступеня;

- дискретні одиниці навчання, шляхом досягнення конкретних цілей навчання, наприклад, шляхом надання кредитів ECTS у вищій освіті;

- конкретний досвід, який сприяє навчанню, наприклад сертифікати, що засвідчують завершення учнівства або іншого досвіду роботи;

- придбання певних навичок, наприклад, через посвідчення, видані у процедурах визнання попереднього навчання;

- досягнення певних критеріїв досконалості, наприклад, отримавши певні призи за досягнення або закінчуючи "з відзнакою";

- конкретний рівень компетентності, досягнутий у конкретних сферах, шляхом видачі сертифікатів про перевірку. Як правило, сертифікати, видані учням, використовуються зацікавленими сторонами, які зацікавлені в отриманні свідчень про навички особи. Наприклад: навчальні заклади це зацікавлені у визначенні придатності індивіда до прогресу на інший рівень освіти; рекрутери та потенційні роботодавці зацікавлені визначити придатність кандидата для відкритих можливостей працевлаштування. Також сертифікація може використовуватися як мотиваційний інструмент в освіті шляхом надання сертифікатів для досягнення конкретних проміжних цілей навчання. Показано, що ця постійна форматова оцінка та сертифікація покращують концентрацію, відгуд та загальні результати навчання.

1.5 Використання сертифікатів для акредитації

Акредитація - це процедура, згідно з якою авторитетний орган дає офіційне визнання того, що орган чи особа є компетентними для виконання конкретних завдань. Акредитація зазвичай засвідчується посвідченням. У освіті використовуються різні форми акредитації:

- освітні організації акредитовані, мають ліцензію на діяльність. Приклади такої акредитації включають акредитації, видані урядами

університетам чи школам; та акредитацію, видану компаніями програмного забезпечення до навчальних центрів для навчання конкретних програмних пакетів. На рис. 1 зображено приклад акредитації та кваліфікації у вищій освіті;

- акредитовані спеціальні освітні програми, що дозволяються до викладання в межах акредитованих освітніх організацій;

- вчителі часто акредитуються за певними навичками, для підтвердження того, що вони є компетентними вчителями та можуть викладати в навчальних закладах;

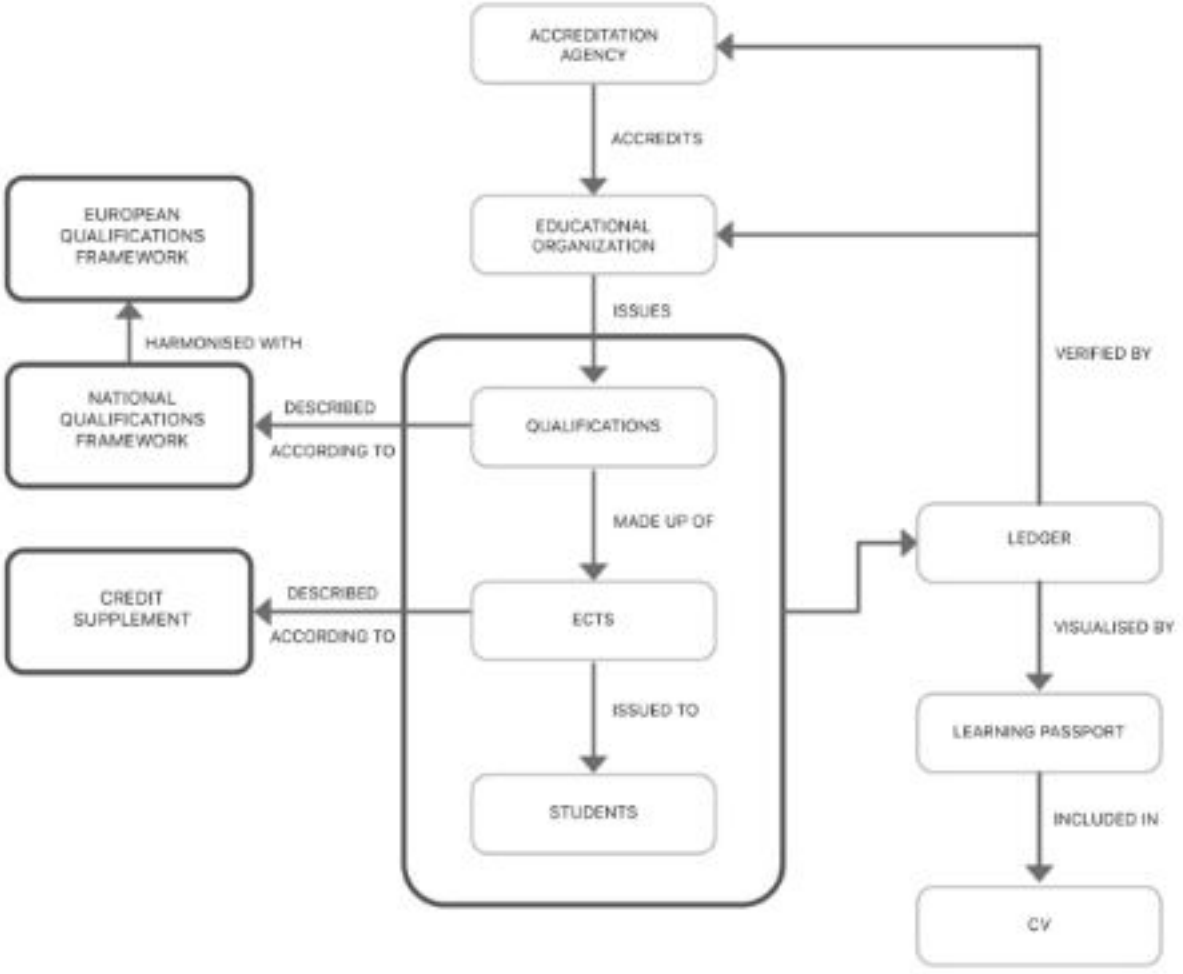


Рис. 1 - Приклад структури акредитації та кваліфікації у вищій освіті

- агентства, які займаються акредитацією, самі акредитують наглядові установи високого рівня, які гарантують, що вони видають свою акредитацію відповідно до встановлених правил. Прикладом такої акредитації є присудження Європейським реєстроєм якості EQAR. Багато цих сертифікатів та

акредитацій, як правило, пов'язані з мережами акредитації. Таким чином, наприклад, студенту може бути наданий сертифікат, який засвідчує ступінь, лише якщо він був виданий за акредитованою програмою, яка у свою чергу була видана акредитованим університетом, який, у свою чергу, був акредитований акредитованою агенцією з якості.

1.6 Використання сертифікатів для відстеження інтелектуальної власності

Реєстрація та відстеження інтелектуальної власності є ключовою частиною всіх академічних систем. Інтелектуальна власність створює цінність, і в свою чергу її використання може покривати витрати. З цією метою велика кількість центральних органів влади використовується для управління різними видами інтелектуальної власності. Зокрема:

- дослідницькі журнали засвідчують, що частина досліджень є новою та що дослідження проводиться відповідно до наукових стандартів - ця інформація використовується для визначення наукової істини;

- компанії підтверджують, скільки разів було використано частину дослідження або відкритий освітній ресурс. Це використовується для визначення значущості дослідження або відкритого освітнього ресурсу, і часто для грошової компенсації автору відповідно;

- патентні відомства засвідчують першого винахідника і надають їм монополію на ринок для отримання прибутку від цього винаходу протягом зазначеної кількості років.

Сертифікати також широко використовуються з фінансових причин, у тому числі для відстеження надходження платежу, нагородження студентських грантів, нагородження студентських кредитів, відмови або внесення змін до студентських позик.

1.7 Обмеження сучасних систем сертифікації

Більшість записів все ще видаються на паперовому або іншому фізичному форматі, хоча зусилля урядування та промисловості по оцифруванню

поширюються по всьому світу. Не існує "ідеального формату" для сертифікатів, при цьому багато країн використовують гібридні сертифікати, за допомогою яких паперові сертифікати підтримуються цифровими базами даних. Проте суттєві обмеження кожної системи явно свідчать про необхідність кращої, більш надійної технології сертифікації.

Сертифікати на паперових документах як і раніше розглядаються в якості найбільш безпечної форми сертифікації, оскільки:

- їх важко підробити через функції безпеки, вбудовані в сертифікати;

- безпосередньо такий сертифікат перебуває у одержувача, який таким чином повністю контролює його;

- відносно безпечно зберігати протягом тривалих періодів часу, наприклад зберігаючи їх у сейфі;

- вони можуть бути представлені адресатом будь-де, будь-якій людині з будь-якою метою.

Однак паперові сертифікати також мають значні недоліки:

- хоча важко підробити, сертифікат не захищений від ризику підробки. Таким чином, емітент зобов'язаний зберігати центральний реєстр виданих сертифікатів, який може бути використаний для підтвердження автентичності сертифіката;

- реєстри сертифікатів єдині засоби підтведження сертифікату, тому під час відмови системи, в той час, як сертифікати можуть залишатися дійсними, можливість їх перевірки втрачається;

- ведення такого реєстру, а також підтвердження дійсності сертифікатів - це ручний процес, який вимагає значних людських ресурсів;

- особливості безпеки в фізичному сертифікаті випливають винятково з рівня складності та експертизи, необхідних для автора документа. Чим безпечніше сертифікат, тим дорожче це виробляти. Захисні сертифікати, такі як паспорти, зазвичай виготовляються за певну грошову суму;

- немає жодних обмежень на здатність емітента змінювати дату видачі або інші відомості про сертифікат;

- неможливо скасувати сертифікат, якщо власник не відмовляється від його контролю;

- якщо третій стороні потрібно використовувати сертифікати, наприклад, для перевірки навичок у резюме вони повинні прочитати та перевірити кожен сертифікат окремо та вручну, що значно впливає на тривалість процесу.

Цифрові сертифікати мають багато переваг перед паперовими сертифікатами:

- вони вимагають набагато менших ресурсів для випуску, обслуговування та використання, оскільки достовірність сертифікатів може бути перевірена з реєстру автоматично, без втручання людини;

- якщо сторонній стороні потрібно використовувати сертифікати, їх можна автоматично порахувати, перевірити та навіть підсумувати, якщо вони видані у стандартному форматі;

- безпека сертифіката випливає з безпеки криптографічних протоколів, які гарантують, що сертифікат дешево виробляти, але надзвичайно важко, або навіть неможливо, для відтворення іншою стороною, крім емітента;

- сертифікати можуть бути відкликані емітентом;

- деякі види шахрайства емітента, такі як зміна мітки часу або зміна серійного номеру сертифіката, можуть бути неможливими або потребувати великих технічних витрат в залежності від конструкції системи.

Проте цифрові сертифікати також мають значні недоліки, а саме:

- без використання цифрових підписів, вони надзвичайно легко підробляються;

- коли використовуються цифрові підписи, для цього потрібні залучення сторонніх постачальників сертифікатів для забезпечення цілісності транзакції; ці сторони мають значний контроль над усіма аспектами процесу сертифікації

та перевірки, під час яких можуть виникнути правопорушення, зловживання таким доступом;

- у багатьох країнах не існує універсального відкритого стандарту для цифрових підписів, що призводить до отримання сертифікатів, які можуть бути перевірені лише в контексті конкретних програмних екосистем;

- легше знищити електронні записи - зберігаючи їх безпечно, потрібні складні, багаторівневі резервні системи, які схильні до збою;

- якщо реєстр не працює, самі сертифікати стають марними, оскільки на відміну від паперових сертифікатів вони не мають власного значення без реєстру;

- реєстри цифрових сертифікатів схильні до великомасштабних витоків даних.

Висновок до розділу

Цифрові документи можуть бути так само ефемерними, як і папір. Вони часто видаються емітентом для одержувача у спеціальних форматах, які без правильного програмного забезпечення неможливо прочитати або перевіряти їх валідність. Навіть при доступі до правильного програмного забезпечення, у багатьох випадках процес підтвердження може бути довготривалим та неточним. Те саме стосується цифрових підписів: навіть в тих місцях, де законодавство передбачає їх прийняття, цифрові підписи входять у широкий діапазон форматів з різним рівнем безпеки, не всі з яких відповідають юридичним нормам.

Ще однією проблемою з цифровими документами є те, що електронна пошта є одним із основних способів, через який люди діляться інформацією в цифровій формі, зазвичай такий спосіб не захищений від викрадення персональної інформації, тому необхідно створювати приватні інфраструктури передачі для надсилання конфіденційних документів, таких як медичні записи, ідентифікаційні документи та інша персональна інформацію.

Також, як і паперові документи, цифрові документи можуть бути підроблені досвідченими шахраями навіть якщо сертифікат має багато рівнів захисту.

Тому сучасна система сертифікації потребує розробки нових методів видачі, сертифікування та підтвердження різних цифрових даних, які потрібно зберігати та передавати між різними сторонами. Така система потребує високої надійності і довіри користувачів, зацікавлених в сертифікації та підтвердженні валідності даних. Головною метою даної роботи є підвищення надійності системи сертифікації, довіри до процесу сертифікації, перевірки валідності сертифікованих даних за допомогою блокчейн технології та зберігання і обмін конфеденційними даними без централізованої системи. Об’єктом дослідження є система сертифікації даних за допомогою блокчейн технології. Предметом дослідження є процес, моделі та методи сертифікації, алгоритми підпису та підтвердження сертифікованих цифрових даних.

РОЗДІЛ 2. ХАРАКТЕРИСТИКИ СИСТЕМИ СЕРТИФІКАЦІЇ ЗА ДОПОМОГОЮ БЛОКЧЕЙН ТЕХНОЛОГІЇ

Технологія блокчейн підходить як нова інфраструктура для захисту, обміну та перевірки навчальних досягнень. У випадку сертифікації блокчейн може зберігати список емітента та одержувача кожного сертифікату разом із підписом документа у відкритій базі даних, яка ідентично зберігається на тисячах комп'ютерів у всьому світі. Цифрові сертифікати, які, таким чином, захищені, мають значні переваги перед "звичайними" цифровими сертифікатами, у тому числі: вони не можуть бути підроблені - можна з точністю підтвердити, що сертифікат був спочатку виданий та отриманий тими самими особами, які вказані в сертифікаті; перевірка сертифіката може виконуватися програмним забезпеченням з відкритим кодом будь-ким, хто має доступ до блокчейну; відсутність необхідності для будь-яких посередників. Також механізм такого цифрового сертифікату дозволяє підписувати документ для публікації, не вимагаючи публікувати сам документ, таким чином зберігаючи конфіденційність документів.

Блокчейн відповідає наступним вимогам до сертифіката з точки зору одержувача: він володіє сертифікатом і не вимагає від емітента або сторонніх осіб додаткової перевірки, також він може підтвердити право власності на сертифікат. Виданий сертифікат для одержувача - це постійна реєстрація, яку не можливо підробити, змінити або видалити без відомо всіх учасників блокчейн мережі.

З точки зору емітента блокчейн відповідає наступним вимогам до сертифіката: він може довести видачу посвідчення та встановити термін придатності для посвідчення, крім того він може відкликати посвідчення.

Всі рішення для цифрової сертифікації використовують систему цифрових підписів для видачі сертифікатів. Цифрові підписи можуть бути використані для перевірки того, що конкретний документ був дійсно

підписаний певною особою. Цифровий підпис забезпечує спосіб видачі сертифікатів, дозволяючи особі позначити документ штампом, який тільки вони можуть генерувати та переконатися, що документ не може бути підроблений після його підписання.

Так як сертифікат заноситься у блокчейн мережу, яка виступає гарантом надійності та валідності даних, третя сторона може довіряти освітнім даним, які знаходяться у мережі без попередньої перевірки. Якщо все ж таки третя сторона бажає підтвердити валідність сертифікату, вона повинна знати відкритий ключ особи, яка підписала документ. Програмне забезпечення перевірки працює шляхом введення документа та відкритого ключа, після чого перевіряє, що підпис у документі відповідає хешу оригіналу документа та що підпис документа математично пов'язаний з відкритим ключем особи, яка стверджує, що підписав документ зі своїм приватним ключем. Оскільки сертифікати, збереженні в блокчейні, можуть бути автоматично підтверджені, освітні організації більше не повинні витрачати ресурси на підтвердження валідності освітніх досягнень, значно зменшуючи їх адміністративне навантаження.

Таким чином, технологія блокчейн дає можливість створити надійну, безпечну та довірчу систему, яка працюватиме без посередників при видачі та підтвердженні освітніх досягнень. Деякі престижні інститути вже використовують системи для забезпечення цифрових сертифікати, такі як: Blockcerts, BADGR та Mozilla Open Badge. Технологія блокчейн вирішує основу проблему підроблення сертифікатів та інших освітніх досягнень.

2.1 Огляд блокчейн технології та книг обліку

Блокчейн - це розподілений обліковий запис, який забезпечує спосіб запису інформації та спільного використання спільнотою в мережі. У цій системі кожен учасник зберігає свою власну копію інформації, і всі члени повинні підтвердити будь-які оновлення колективно. Інформація може являти собою транзакції, контракти, активи, ідентифікаційні чи практично щось інше,

що можна описати в цифровій формі. Записи є постійними, прозорими та доступними для пошуку, завдяки чому члени системи можуть переглядати всю історію транзакцій. Кожне оновлення - це новий "блок", доданий до кінця "ланцюжка". Протокол керує тим, як ініціюються, перевіряються, фіксуються та розподіляються нові редагування або записи. За допомогою блокчейна криптологія замінює сторонніх посередників тим самим підвищуючи довіру та цілісність системи.

З початку 1990-х років проводилися експерименти з блокчейном, але тільки в 2008 році блокчейн технологія отримала широке застосування. Першим відомим блокчейном став біткойн система, яку також називають першою широко використовуваною децентралізованою криптовалютою. Біткойн також відноситься до мережевого протоколу, що лежить в основі криптовалюти. З точки зору використання, біткойн блокчейн автоматично асоціюється як основна блокчейн система, коли на практиці існують й інші не менш важливі та популярні системи, такі як блокчейн етеріум.

Основним компонентом блокчейну є книги обліку, за допомогою яких можна визначити власника активу в будь-який момент часу. У системі, яка використовує обліковий запис для визначення власності на певний актив для передачі права власності між двома сторонами потрібно зробити запис у книзі обліку.

З технічної точки зору, книга обліку - це просто список послідовних транзакцій з часовим штампом. Для прикладу на рис. 1 наведений один із варіантів запису транзакцій.

Ця проста ідея збереження переліку активів дозволяє систематично переносити і накопичувати інформацію та банк даних. Людина або організація, яка фізично володіє або контролює загальну книгу, в тому числі сервер, на якому розташована книга, у випадку онлайнової облікової книги, має значну силу та вплив. Зокрема, власник книги може:

- вирішити, чи потрібно записувати транзакцію, яка в свою чергу дає цій особі можливість: нав'язувати особам умови для реєстрації своїх операцій і прийняття рішення щодо системи контролю, яка буде застосована для перевірки точності цих операцій;

- змінювати або видаляти транзакції, що вже знаходяться в книзі обліку;

- повністю знищити книгу або дозволити її знищити.

TRANSACTION NO.	DATE & TIME	SENDER	ASSET	RECEIVER
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2
#	dd-mm-yy hh:mm	Person 1	Description of asset transfered e.g. a unit of currency, a deed toa property or a certificate.	Person 2

Рис. 2 - Варіант запису транзакцій

Особу або організація, яка контролює такі книги, має значний вплив, навіть просто зберігаючи реєстр транзакцій. Загалом власник такої системи відповідає за створення, зміну або видалення транзакції з книги обліку, а також може здійснювати зміну власності на актив. Відповідальність за точність ведення обліку традиційно покладається на різні установи: уряди контролюють право власності на землю, керуючи бухгалтерією власності; банки контролюють світову грошову систему шляхом проведення валютних операцій; фондові біржі контролюють великі частки ділового світу, зберігаючи рахунки для власності бізнесу. Оскільки капіталістичні суспільства будуються навколо концепцій продажу та власності, передача та накопичення капіталу, існують великі обов'язки та ризики, пов'язані з зберіганням таких книг обліку великих обсягів конфіденційної інформації.

Зокрема, ці центральні органи влади мають такі загальні вимоги: надавати свідків - тобто, засвідчити особистість та забезпечити, щоб особи були записані в облік; бути чесним і прозорим у всіх операціях, тобто не позбавляти користувачів своїх активів, створюючи фальшиві транзакції або незаконно змінюючи транзакції після їх створення; забезпечувати безпеку, тобто гарантувати, що неавторизовані сторонні особи не можуть читати та писати в книзі обліку; не зловживати своєю монополією шляхом введення несправедливих/виняткових витрат на їх послуги; дозволяти особам здійснювати транзакції - тобто надавати доступ усім, хто має законний інтерес для здійснення транзакцій, перерахувавши їх у книзі обліку.

Наслідком цього є те, що ці інституції можуть індивідуально чи колективно завдати значної шкоди або навіть соціального хаосу, зловживаючи довірою, яка надається їм для точного ведення та підтримки цих книжок. Висновок полягає в тому, що ці інститути мають повноваження використовувати або зловживати своїм контролем над книгами та здійснювати значний контроль над окремими особами та суспільствами в межах своєї безпосередньої компетенції.

Найбільш відоме застосування блокчейна - це публічна книга операцій з криптографічними валютами, такими як біткойн та ефір. Як і у випадку з іншими публічними книжками, обліковий запис містить відомості про походження та передачу права власності на актив. Головна ідея біткойна — створення валюти, яка працюватиме прозоро, вільно поширюватиметься і не знеціниться. На відміну від звичних грошових одиниць, нині жодна держава не може контролювати, додатково «надрукувати» або знецінити біткойни. Таким чином ця криптовалюта має надійний захист від підробки, нею можна миттєво розрахуватися будь-де у світі за наявності підключення до інтернету. Водночас переказ відбувається анонімно і без стягнення комісії банком.

Біткойн нерідко порівнюють з євро або доларом, однак влучнішим було б порівняння із золотом або сріблом, оскільки властивості біткоіна в дечому подібні до властивостей дорогоцінних металів.

Кількість криптовалюти обмежена — загалом випустити або видобути можливо 21 мільйон біткоінів, заразом у світі на сьогодні уже існує близько 16,5 мільйонів.

Транзакційна структура протоколів блокчейнів сприяє не тільки передачі криптовалюти, але й інших цифрових активів. Актив може бути відчутним, наприклад, будинок, автомобіль, готівка, земля або нематеріальні, як інтелектуальна власність, така як патенти, авторські права чи брендинг. Практично будь-яка цінність може відслідковуватися та обмінюватися мережею блокчейн, зменшуючи ризики та скорочуючи витрати для всіх, хто задіяний. Всі блокчейн традиційно мають певну цифрову валюту, пов'язану з ними, за допомогою якої здійснюється запис та збереження транзакції.

Отже, блокчейн загалом є обліковими записами груп транзакцій, інакше вони називаються блоками, які криптографічно пов'язані разом у лінійній тимчасовій послідовності. Інші ключові властивості, пов'язані з блокчейном - це безпека, незмінність, налаштування - ці властивості залежать від архітектури блокчейна та характеру консенсусного протоколу, який він використовує для побудови системи. Деякі блокчейни структуровані для полегшення однорангових транзакцій через неієрархічні вузли, відомо як розподілена мережева структура. Деякі блокчейни, як і біткойн, також забезпечують незмінність своїх записів через свій унікальний консенсусний протокол.

Щоб визначити, хто володіє певним активом, достатньо просто зробити пошук у книзі обліку, щоб перевірити, хто є його останнім власником. При описі блокчейна важливо розуміти як і сукупність соціальних принципів, що лежать в основі його соціальної цінності, так і характеристики його архітектури для підтримки технічної характеристики.

2.2 Соціальна цінність та принципи технології блокчейн

Можна визначити сукупність принципів, які є основою соціальної цінності технології блокчейнів, як грунт для розуміння конкретних можливостей технології блокчейнів у сфері освіти.

Першим принципом блокчейну є здатність особи володіти та контролювати свою власну ідентичність в інтернеті, публічні блокчейн системи сприяють самодостатності, надаючи людям можливість бути остаточним арбітром того, хто може отримати доступ і використовувати їх дані та особисту інформацію. У межах освітньої сфери самоідентичність означає повноваження окремих учнів володіти, управляти та ділитися деталями своїх навчальних досягнень без необхідності навчальному закладу виступами надійним посередником. Також це можна вважати тим, що громадяни набувають значної самоорганізації стосовно того, як особисті дані та ідентичність поширюється в інтернеті, а також отримують можливість ділитися своєю інформацією без необхідності постійного звернення до стороннього посередника для перевірки таких даних чи ідентичності. Прикладом сучасної системи ідентичності можна назвати Telegram Passport, який дозволяє зберігати ідентифікаційний документ та проходити ідентифікацію на портали без необхідності підтвердження документів третьою стороною. На рис. 3 показано, як вноситься інформація в такий додаток.

Цифрова ідентичність поширюється на право людини. Тим не менш, досі не існує надійного способу боротьби з одним з недоліків інтернету - виявлення людей або машин в інтернеті. Коли громадяни зобов'язані або згодні розголошувати свою ідентичність в інтернеті, з’являються нові проблеми, такі як використання приватних алгоритмів для максимального комерційного застосування персональних даних користувачів у соціальних мережах та здобуття прибутку на таргетуванні відповідної реклами. Технологія блокчейн принципово змінює нашу здатність представляти себе. Криптографія в основі

технології блокчейнів вирішує проблеми, пов'язані з недоліками ідентичності, захистом та контролем персональних даних індивідуальному користувачеві.

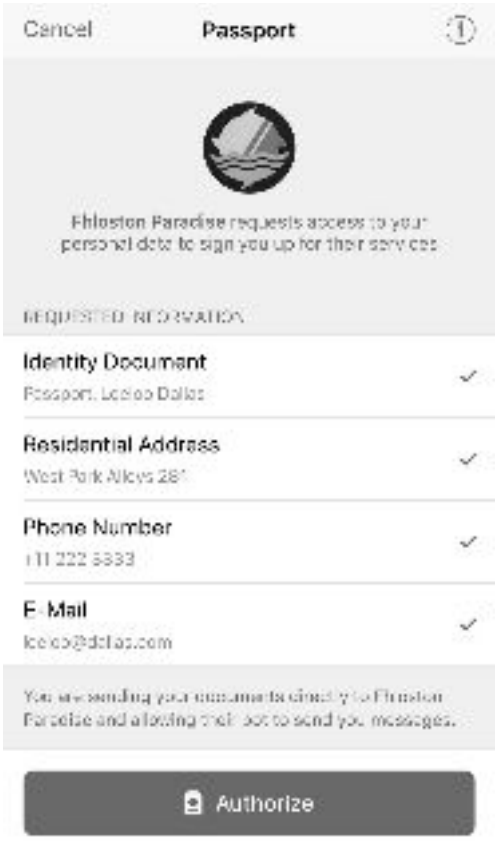


Рис. 3 - Приклад внесення своїх ідентифікаційних даних до блокчейну Telegram Passport

Люди, підприємства та установи можуть зберігати особисті дані на власних пристроях та надавати їх тим, хто повинен перевірити його, не покладаючись на центральне сховище особистих даних. Технологія блокчейн забезпечує новий спосіб оцифрування паперу, який дає нам можливість контролювати свою ідентичність в інтернеті та правильно управляти своїми персональними даними.

Фактично повний цифровий самоконтроль може в кінцевому підсумку дозволити відмовитися від спільного використання постійної ідентичності. Замість цього стане основним стане перевірка претензій. Іншими словами, замість запиту сторонньої інформації сторони запитують лише інформацію, яка

стосується саме цієї операції: чи є особа віком від 18 років? Чи отримали вони ступінь кандидата наук в галузі нейронауки від MIT? Чи є вони громадянами Італії? Після підтвердження претензії можуть бути відхилені або прийняті суб'єктом.

Впливові дослідження різних організацій вказує, що довіра є важливим принципом між двома та більше людьми, організаціями або націями, і що в кіберпросторі довіра грунтується на двох основних вимогах:

- автентифікація - доведіть мені, що ви є саме тим, ким ви себе називаєте;
- авторизація - доведіть мені, що у вас є дозволи, необхідні для того, щоб зробити те, що ви просите.

Якщо одна із сторін не задоволена відповіддю, вони можуть все-таки вирішити дати дозвіл іншій стороні продовжувати транзакцію, але в такому випадку сторона ризикує впустити в систему користувача, який може нанести збиток цілісності системи. Проте, не існує життєздатних відносин, якщо сторони не вірять один одному. У цьому сенсі достовірність у суспільстві є аналогічною кредитоспроможності. Ця основна концепція довіри залишається незмінною в цифровому світі, де ми повинні покладатися на багатьох суб'єктів, котрих ми ніколи не зустрінемо, діяти добросовісно та від нашого імені. Довіру часто надають лише для дуже специфічного застосування в рамках конкретного контексту і протягом певного періоду часу. У світовій цифровій економіці вимоги довіри - з результатами перевірок та противаг - стають дедалі дорожчими, незмінними та неефективними.

Технологія блокчейн може стати життєздатною альтернативою поточній процедурній, організаційній та технологічній інфраструктурі, необхідній для створення інституційної довіри. Підвищена довіра між зацікавленими сторонами пов'язана з використанням децентралізованих облікових записів громадськості, а також криптографічних алгоритмів, які можуть гарантувати,

що затверджені транзакції не можуть бути змінені після їх перевірки. Блокчейн алгоритми досягають підвищення надійності та довіри шляхом автоматизації трьох ролей довіреної третьої сторони: перевірки, безпечних операцій та збереження транзакцій.

В майбутньому так само як інтернет переосмислює комунікацію та впливає на соціальну поведінку, блокчейн може допомогти усунути існуючі прогалини у транзакціях, контрактах та довірі, які є основними принципами бізнесу, уряду та суспільства.

Легкість спільного використання та видимість є важливими ознаками блокчейну. Відсутність однієї з цих функцій у поточних розроблених системах часто є центральним фактором прийняття блокчейн технології. Вони стають особливо критичними у транзакціях, в яких більше ніж одна організація проводить транзакції.

Блокчейн надає учасникам інформацію про походження кожного активу чи запису та про те, як його власність змінилася з часом. Проте ця прозорість функціонує лише тоді, коли транзакції блокчейна пов'язані з ідентифікатором. Без публічного ідентифікатора, такого як пов'язаний документ або серійний номер, транзакції за допомогою блоків не можуть бути декодовані та відстежені. Таким чином, блокчейни - навіть загальнодоступні блокчейни - за замовчуванням є приватними, але можуть використовуватися для відстеження транзакцій окремих осіб з плином часу за допомогою пов'язаних даних в публічних банках даних.

Технологія блокчейн являє собою безперечний механізм для перевірки того, що транзакція виконалася в певний момент часу. Крім того, історія, положення та власність кожного блоку автоматично автентифікуються і не можуть бути змінені, тому що кожен блок у ланцюзі містить інформацію про попередній блок. Єдиний загальний обліковий запис забезпечує одне місце для визначення права власності на актив або завершення певної транзакції.

Незмінний запис - це запис, стан якого неможливо змінити після його створення. Незмінність взаємопов'язана з безпекою та її класичними властивостями конфіденційності, цілісності та доступності. Незмінність полягає також у стійкості та незворотності. Дані блокчейн неможливо легко змінити, оскільки вони постійно зберігаються в багатьох різних місцях. За допомогою криптографії приватного та відкритого ключів, що є частиною базового протоколу блочного кешу, транзакційна безпека та конфіденційність стають практично незмінними.

Незмінність блокчейн ланцюгів означає, що зміни, які потрібно внести після встановлення, практично неможливі, що, в свою чергу, підвищує довіру до цілісності даних та зменшує можливості шахрайства. Для того, щоб транзакція в блокчейні вважалася дійсною, всі учасники транзакції повинні узгоджувати свої вузли, які використовують протокол блокчейн, тобто повинні досягти консенсусу щодо дійсності транзакції. Механізм, за допомогою якого це відбувається, відрізняється в різних архітектурах блокчейну, але, як правило, поширюється в певній мірі, а це означає, що окремий учасник не може бути арбітром правдивості даних в мережі.

Жоден учасник не може втрутитися в транзакцію після того, як вона записана в книгу обліку. Якщо транзакція помилкова, то для виправлення помилки необхідно використати нову транзакцію, і тоді обидві транзакції відображатимуться в книзі обліку. Структура блокчейну розроблена як розподілена мережа вузлів, в яких окремий з цих вузлів зберігає копію цілого ланцюга. Отже, коли транзакція перевіряється та затверджується вузлами-учасниками неможливо змінити дані транзакції. Спроби змінити дані в одному місці будуть тлумачитися як шахрайські та атаки на цілісність інших учасників, внаслідок чого вони будуть відхилені.

Замінивши посередників автоматизованими алгоритмами, блокчейн також підвищує довіру до даних. Учасники блоку пов'язані між собою на ринку,

де вони можуть проводити операції та передавати право власності на цінні активи між собою у прозорий спосіб і без допомоги або втручання сторонніх посередників. Мережа блокчейн працює без певного центрального органу влади. Завдяки технології блокчейнів, алгоритми однорангового консенсусу прозоро записують та перевіряють операції без посередників, тим самим потенційно зменшують або навіть усувають вартість, затримки і загальну складність. Наприклад, блокчейни можуть зменшити накладні витрати, коли сторони торгують активами безпосередньо один з одним або швидко підтверджують право власності чи авторство інформації - це завдання, яке в іншому випадку є неможливим без центрального органу чи неупередженого посередника. Крім того, здатність блоків гарантувати автентичність через інституційні організації, ймовірно, допоможе сторонам зосередити увагу на нових способах аутентифікації записів, вмісту та транзакцій. Велика децентралізація інтернету надасть більше контролю в руки користувачу або пристроїв користувача - замість того, щоб спиратися на платформи хмар, якими керують такі, як Google або Amazon.

2.3 Типи записів для зберігання в блокчейн

Blockchain зазвичай використовуються для зберігання записів про операції з активами, розумні контракти, цифрові підписи та сертифікати.

Першим типом записів в блокчейні можуть бути операції з активами. Звіти про транзакції активів зазвичай приймають у двох формах:

- гроші, виражені в одиницях валюти: кожна одиниця одиниці тієї ж валюти має однакову цінність, як і кожну іншу одиницю в будь-який час. Валюта також є внутрішньо-конвертованою за обмінним курсом. Найпоширенішою формою валюти, побудованої за технологією блокчейнів, є біткойн.

- документальні підтвердження прав власності, юридично відомі як права власності. Вони широко використовуються для представлення нерухомого

майна, такого як земля або нематеріальне майно, таке як права інтелектуальної власності.

Ще одним типом записів в блокчейні можуть бути розумні контракти, які є фактично невеликими програмами, що зберігаються в блокчейні, які виконують транзакцію за вказаних умов. Таким чином, розумний контракт - це, як правило, така декларація, яка зберігає "переміщення X в Y, якщо відбувається Z". На відміну від звичайного контракту, коли після досягнення домовленості сторони повинні виконати договір про його проведення, розумний контракт самостійно виконується - тобто після того, як інструкції будуть записані в блокчейн, транзакція буде відбуватися автоматично, коли відповідні умови виявлені, без будь-яких подальших дій, необхідних сторонами угоди, або інших третіх сторін.

Цінність представлена розумними контрактами, полягає в тому, що після того, як важливі цифрові записи будуть автоматично перевірятися та вноситися, вся нова екосистема технічної автоматики почне розвиватися, щоб дозволить створити нову соціальну структуру, яка забезпечить громадянську ефективність, особисту мобільність та інституційні перетворення. У цьому контексті інтелектуальні контракти представляють автоматичний погляд на майбутнє.

Також типом записів в блокчейні можуть бути сертифікати та цифрові підписи. У загальній формі сертифікація є питанням заяви від однієї сторони до іншої, що певний набір фактів є вірним. Підписи є доказом того, що заява була випущена від однієї сторони до іншої. Блокчейни можуть використовуватися як для зберігання криптографічних хешей (цифрових штампів) сертифікатів, так і для зберігання самих сертифікатів. Таким чином, блокчейн може взяти на себе функцію реєстру державних сертифікатів.

2.4 Огляд високорівневої архітектури блокчейн

Кожна особа, яка бажає торгувати будь-яким активом через приватну або загальнодоступну мережу, має отримати доступ до мережі. Цей доступ здійснюється за допомогою програмного додатку, що зв’язує користувача та блокчейн. Програмний додаток, який часто називають "гаманцем", можна встановити безпосередньо на пристрій або отримати доступ через веб-браузер. Приклад такого додатка зображено на рис. 4. Залежно від призначення, блокчейн гаманець може використовуватися для надсилання та/або отримання цифрових активів. Деякі гаманці дозволяють здійснювати прямі операції без сторонніх посередників, тоді як інші додатки управляються третіми сторонами, які зберігають цифрові активи користувачів від їх імені.

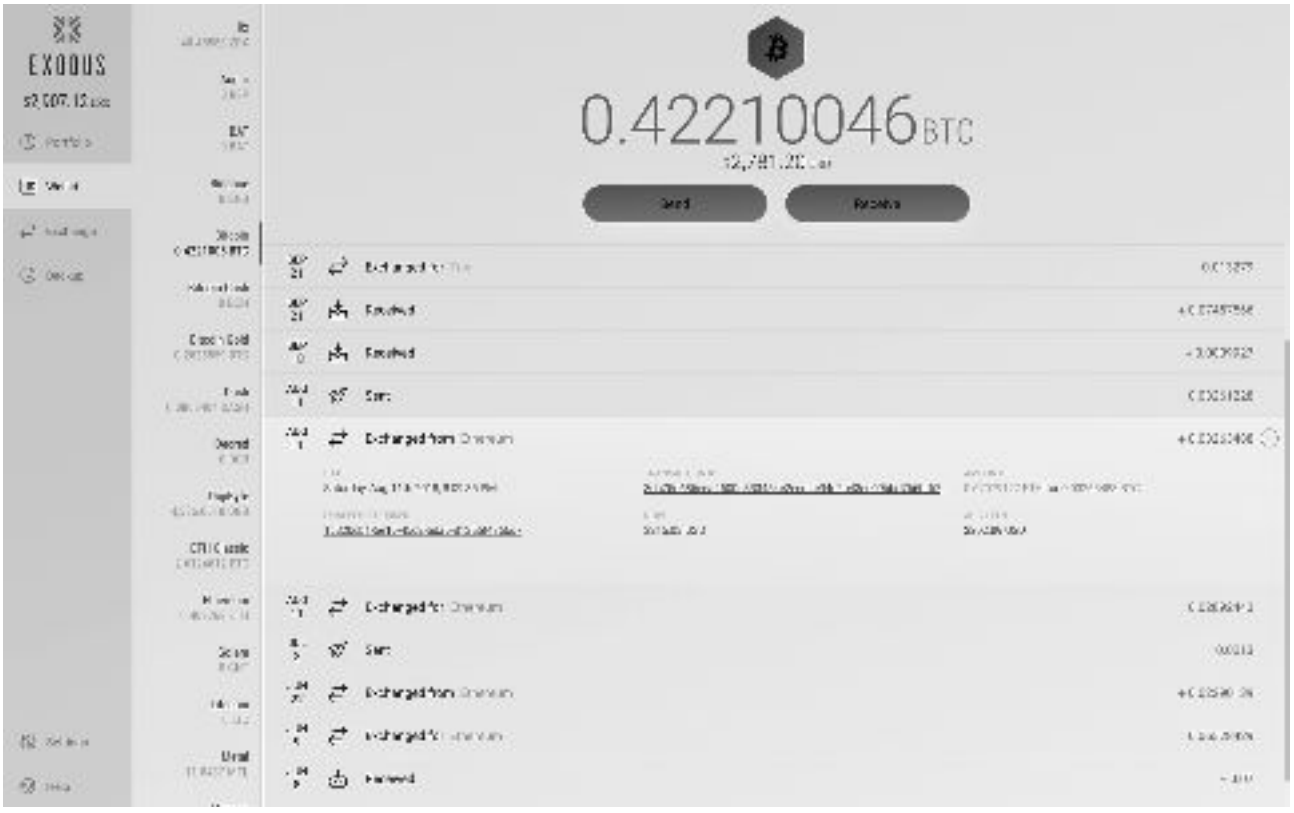


Рис. 4 - Приклад блокчейн ‘гаманця’ Exodus

Користувачам, які бажають брати участь у перевірці транзакцій за допомогою консенсусу, загалом слід встановити програмне забезпечення блокчейну на своєму пристрої. Це використовується для запису в книгу обліку, зберігання цілісності копії всієї книги та збереження всіх копій книг в постійній

синхронізації. Оскільки загальнодоступні блокчейни дозволяють будь-кому інсталювати програмне забезпечення та мати копію всієї книжки, кожен може здійснювати транзакцію безпосередньо на блокчейн всередині мережі, та треті сторони не можуть встановлювати умови для доступу до системи. У приватних блокчейн системах централізований орган визначає, хто має доступ до запуску вузла та участі в процесі консенсусу.

Списки транзакцій або блоки в блокчейні зв'язуються разом криптографічно, що робить їх захищеними від несанкціонованого доступу. На відміну від записів у цифрових базах даних, які можуть бути змінені, після того, як транзакція буде записана та закріплена часовою міткою в блокчейні, її неможливо змінити або видалити.

Блокчейн записує факт транзакції, тобто те, що було передано, сторони, що беруть участь, а також структуровану інформацію (метадані), пов'язану з транзакцією та криптографічний хеш (цифровий штамп) змісту транзакції. Цей унікальний підпис використовується для підтвердження транзакцій, коли хтось змінює вміст транзакції, його одержаний унікальний код більше не відповідає версії, яка входить в ланцюжок, і програмне забезпечення блокчейнів визначить невідповідність.

Усі сторони, що беруть участь у транзакції, і лише ті сторони, повинні домовитись про досягнення консенсусу перед тим, як до мережі додадуть нову транзакцію. Всі інші вузли в мережі лише підтвердять, що обидві сторони мають відповідну здатність вступати в транзакцію. Таким чином, як тільки одна сторона погоджується надіслати актив, а інша сторона погоджується отримати актив, а вузли перевіряють, чи є кожна сторона здатною провести транзакцію, вона завершена.

Всі комп'ютери в мережі постійно та математично перевіряють, чи їх копія блокчейна ідентична всім іншим копіям у мережі. Версія, що працює на більшості комп'ютерів, вважається ‘справжньою’ версією, тому єдиним

способом змінити записи є контроль над половиною комп'ютерів у мережі. Для блокчейнів, що працюють на тисячах, або мільйонах, комп'ютерів, як і загальнодоступні блокчейни, такі як біткойн та етеріум, зміна запису або контроль мережі може бути майже неможливим завданням. Для знищення книги блокчейн система потребує видалення кожної його копії в світі.

2.5 Архітектура блокчейну

Централізований бухгалтерський облік - це єдиний авторитетний список записів транзакцій. Прикладом цього може бути національний реєстр земель. З точки зору комп'ютера централізована база даних зберігається і виконується на одному центральному вузлі. Варіація централізованого обліку, з елементом розподілу, включає кілька вузлів системи, які поділяють відповідальність за різні частини єдиного авторитетного бухгалтерського обліку. Таким чином, розглянемо національний реєстр земель, який управляється регіональними відділеннями, кожен з яких лише обробляє та зберігає операції у межах своєї юрисдикції, але всі вони, в кінцевому підсумку, складають єдину базу даних національних земельних угод. У комп'ютеризованому виконанні цього, кожен вузол лише зберігає свою частину бази даних і виконує свою частину коду. Якщо центральний комп'ютер виходить з ладу, доступ до його бухгалтерії блокується. Децентралізація та розповсюдження облікової книги передбачає повністю вилучення центрального контролюючого органу шляхом створення системи, яка передбачає:

- декілька осіб зберігають копії всієї книжки;
- написання або внесення змін до книги вимагає консенсусу від осіб, які мають копії;
- кожне додавання або зміна записується у кожній копії книги - таким чином, кожна копія однаково авторитетна.

Для створення унікального ідентифікатора блокчейн використовує хеш функцій. Хеш - це короткий код заданої довжини, який служить відбитком для

цифрового документа. Програма, яка називається хеш-генератором, дозволяє користувачеві завантажувати будь-який рядок тексту і створювати унікальний ідентифікатор (рис. 5). Кожного разу, коли один і той же рядок тексту запускається через хеш-генератор, він дасть той самий ідентифікатор документа. Хешування впливає на надійність та захищеність системи, так як якщо змінюється одна буква в документі, вона автоматично генерує зовсім інший ідентифікатор. Хеш є одностороннім - це означає, що хеш-генератор може використовуватися для створення хешу з документа, але математично неможливо згенерувати документ з хешу.

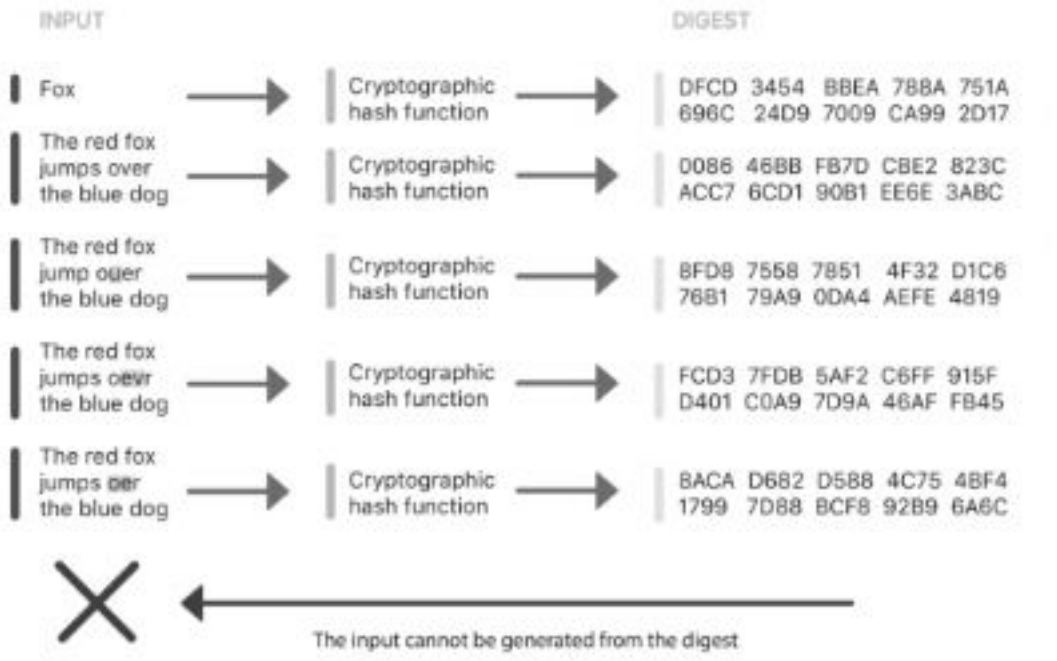


Рис. 5 - Приклад хеш-генератора

У блок-схемі кожен блок транзакцій забезпечується шляхом включення хешу інформаційного блоку, а також попереднього блоку, що дозволяє всім сторонам гарантувати, що жодна з транзакцій не була модифікована чи не була підроблена.

Для підпису транзакцій блокчейн використовує публічні/приватні ключі. Публічний ключ фактично є загальнодоступним ідентифікаційним номером, який можна використовувати для ідентифікації особи. Приватний ключ є фактично пароль, який був математично пов'язаний з відкритим ключем.

Використовуючи пари публічних/приватних ключів, користувач може автентифікувати, що він дійсно є власником відкритого ключа, вводячи їхні дані приватного ключа в програмне забезпечення; це, в свою чергу, перевірить, чи дійсно два ключі пов'язані математично. Ця функція не може бути практично запущена в зворотному порядку - тобто майже неможливо генерувати приватний ключ, якщо в ньому є лише інформація про відкритий ключ.

Блокчейн використовується для реєстрації торгівлі цифровими активами. Найбільш базовим активом, операції якого вбудовані в роботу більшості протоколів блокчейнів, є криптовалюта у вигляді жетонів, таких як біткойн, ефір, лайткойн та інші. Однак вони також можуть бути використані для обміну іншими активами, такими як земельні ділянки або ідентифікаційні документів.

Кожна блокчейн мережа має різні правила щодо того, які активи торгуються, і в яких умовах відбувається торгівля. Ці правила кодуються в його програмному забезпеченні. Кожен пристрій, що працює на програмному забезпеченні блокчейн, відомий як вузол і підключений до мережі вузлів, що запускають цю програму. Коли будь-хто може налаштувати вузол і здійснювати транзакцію безпосередньо з будь-яким іншим вузлом у мережі, це відоме як загальнодоступна мережа блокчейн.

Однак, якщо пристрій підключено до внутрішньої мережі, тобто до приватної мережі, до якої належать лише певні пристрої, то може відбуватися торгівля між вибраною групою осіб, яким було надано доступ до цієї мережі. Це відоме як приватна мережа блокчейн.

Архітектура блокчейн програмного забезпечення гарантує, що тільки ідентичні копії програмного забезпечення можуть взаємодіяти один з одним. Тому, якщо хтось змінює копію програмного забезпечення, вони ефективно створюють абсолютно новий блокчейн. Це відоме як "вилка". З моменту введення в дію протоколу біткойн в 2009 р. було декілька вилок програмного

забезпечення блокчейнів: у серпні 2017 р. виникла вилка біткойн під назвою біткойн кеш.

Протокол ідентифікації гарантує, що всі пристрої в мережі діють за однакових умов, без потреби центрального органу влади, який перевіряє, що дотримуються правила встановлені програмним забезпеченням. На рис. 6 зображено приклад того, як блокчейн працює.

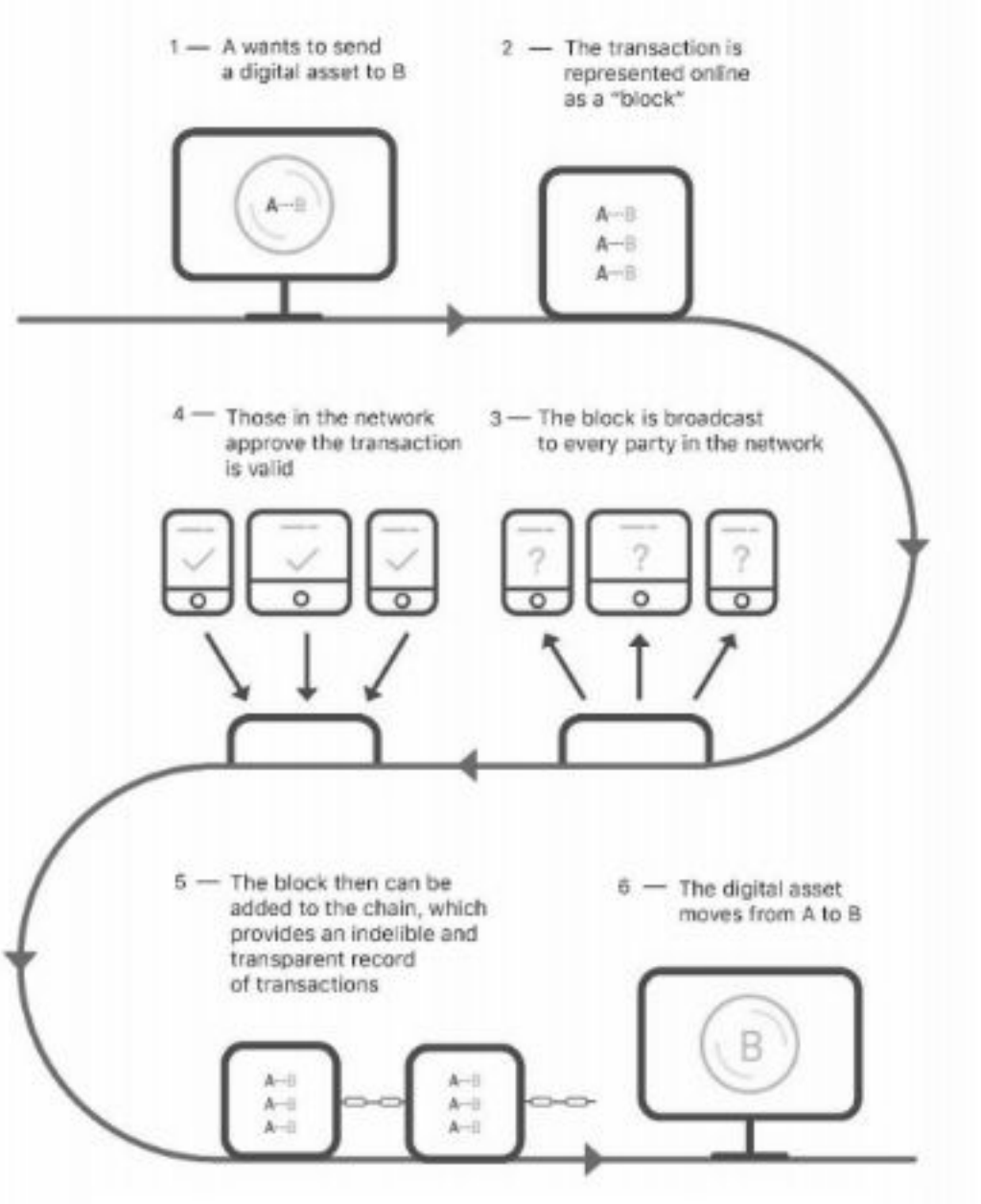


Рис. 6 - Приклад роботи блокчейн

В основі кожного блокчейн є прозорий і автономний децентралізований бухгалтерський облік. Кожен вузол мережі блокчейн:

- зберігає повну копію книги;
- записує нові записи до свого обліку, коли отримує консенсус (підтвердження) від решти мережі;
- транслює транзакції, здійснені її користувачем до іншої частини мережі, для перевірки консенсусу та створення нового запису;
- регулярно перевіряє, чи його копія книги є тотожною, до інших частин мережі.

Програмне забезпечення блокчейн може видати особу з адресою біткойну, яка пов'язана з їх унікальним відкритим ключем та його криптографічно пов'язаним приватним ключем.

Щоб створити нову транзакцію у блокчейні, тобто передати актив, пов'язаний з адресою біткойна, користувач повинен ввести таємний приватний ключ, пов'язаний із цією відкритою біткойн-адресою, яка була випущена при першому запуску програмного забезпечення (рис. 7).

Рис. 7 - Приклад транзакції

Право власності на активи, які були переведені на конкретну адресу біткойн, перевіряються за допомогою приватного ключа.

Таким чином, так як і сторони, що беруть участь у транзакції, так і громадськість можуть бачити, що транзакція відбулася. Кожен із цих учасників транзакції може потім використовувати свої активи, просто вводячи їх приватний ключ у програмне забезпечення біткойн, не вимагаючи доведення або виявлення своєї ідентичності будь-якій сторонній стороні або посереднику (рис. 8).

Таким чином, кожна нова транзакція додається до блоку, тоді як кожен блок прикріплений до попереднього блоку, який утворює ланцюжок. Цілісність ланцюга забезпечується за допомогою двох наборів хешування (рис. 9):

- всі транзакції в межах блоку стискуються та прив'язуються до блоку за допомогою спеціальної хеш-функції, яка називається коренем Merkle. Цей хеш входить до заголовку блока.
- заголовок кожного блоку також включає хеш всієї інформації в попередньому блоці.

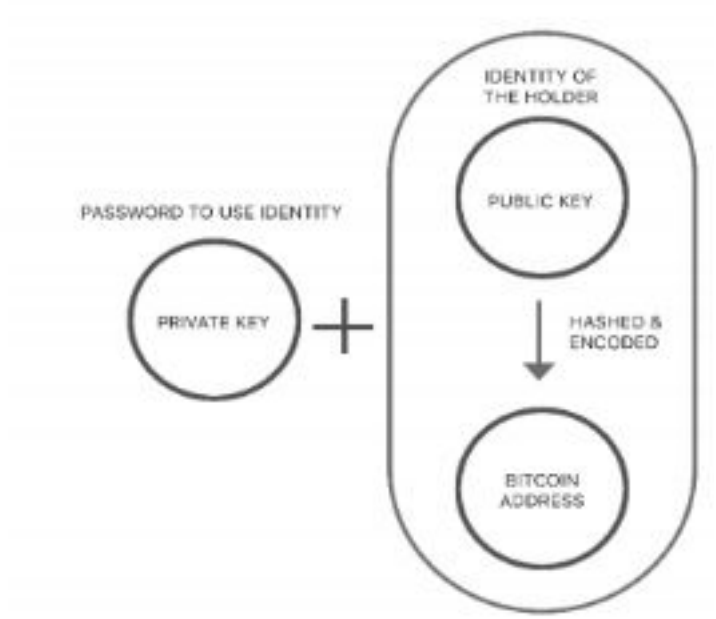


Рис. 8 - Підписування біткойн транзакції

Коли хтось намагався відредагувати одну з транзакцій у ланцюжку, хеш наступного блоку одразу стає недійсним. Таким чином, зламати ланцюжок вимагатиме не тільки зміни транзакції, але також перерахунок і зміна заголовків інформації кожного блоку, створених з цієї транзакції. Зміна однієї транзакції призводить до того, що книгу обліку потрібно оновити на більш ніж половину комп’ютерів у мережі, така операціє занадто складна та вимагає багато ресурсів.

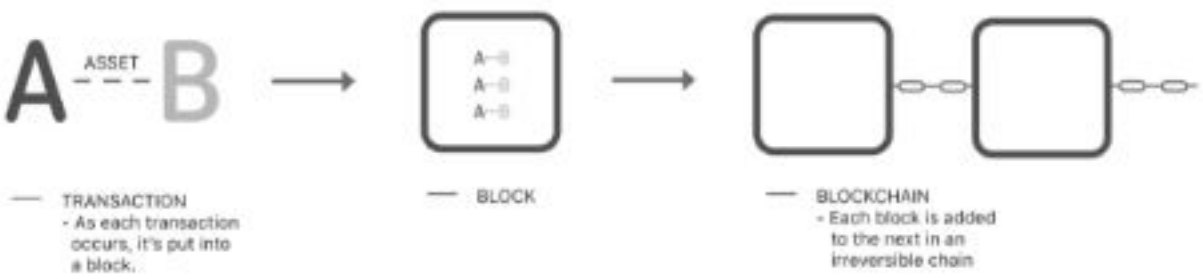


Рис. 9 - Побудова блокчейн ланцюга

Для великих блокчейн систем практично неможливо змінити будь-які транзакції, оскільки це вимагатиме непрактично великих обсягів обчислювальної потужності для цього коли кількість блоків у ланцюзі постійно зростає, кількість обчислювальних потужностей, необхідних для внесення такої зміни, також постійно зростає. Це важливий аспект досягнення обчислювальної потужності раптово поставлять під загрозу безпеку блокчейну або зроблять її застарілою.

2.5 Цифрові сертифікати з використанням технології блокчейн

Технологія Blockchain підходить як нова інфраструктура для захисту, обміну та перевірки цифрових сертифікатів.

Там, де сертифікат може мати вимірюване значення, він може бути представлений як токен і зберігатися безпосередньо в спеціальному блоці. Таким чином, наприклад, на блокчейні для:

- сертифікатів про закінчення школи, єдиний сертифікат може розглядатися як один токен;
- освітні кредити, 1 ECTS буде дорівнювати одному токену;
- відстеження посилань на журнальні папери, одне посилання може дорівнювати одному токену.

Таким чином, сертифікати можуть передаватися від однієї людини до іншої, просто транзакцією токенів в блокчейні. Додаткова інформація про сертифікат може бути збережена або безпосередньо в блокчейні, або зберігатися в вхідному блоці. Таким чином, можна спроектувати базу даних, де

деяка інформація була б приватною та зберігалася користувачем, а інша інформація була б відкритою для блокчейну.

Перевага випуску сертифікатів безпосередньо в блокчейні полягає в тому, що самі сертифікати, а не лише докази їх підписання стають незмінними і постійними.

Недоліком є те, що будь-який блокчейн загального призначення почне масштабуватися, тому значно зросте використання ресурсів підтримки такої системи, що призведе до низької продуктивності. Таким чином, така модель може бути реалізована лише як приватний блокчейн.

Всі рішення для цифрової сертифікації використовують систему цифрових підписів для видачі сертифікатів (рис. 10). Цифровий підпис відрізняється від електронного підпису, що є просто традиційним підписом, тільки підписаний на електронному пристрої в електронному документі (наприклад, електронною ручкою) або відсканованим фізичним підписом.

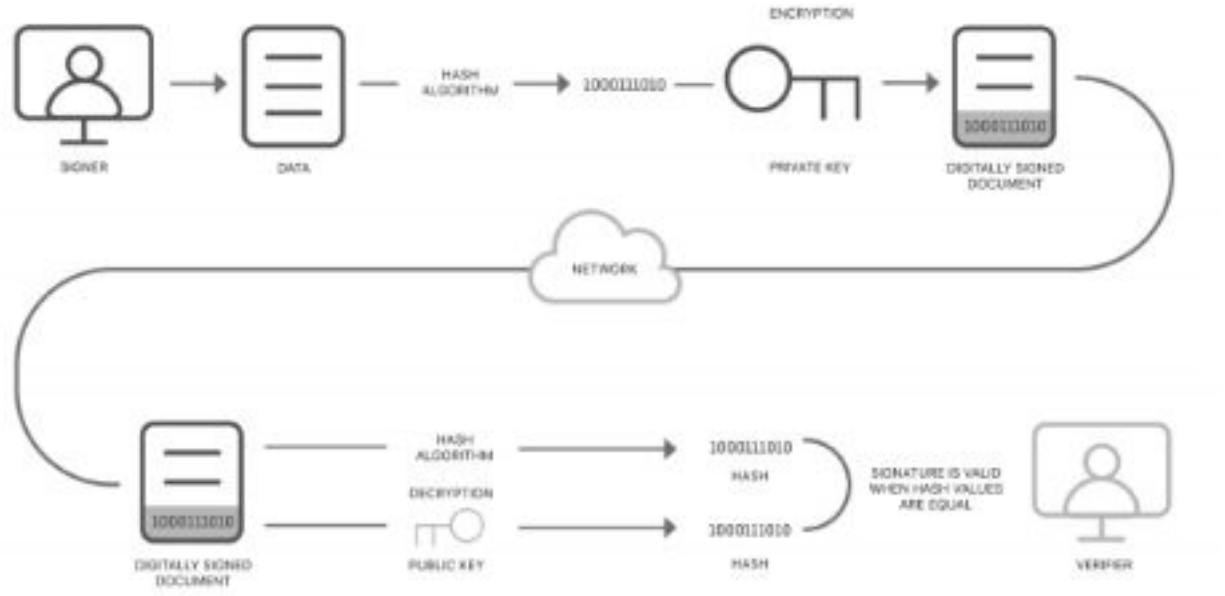


Рис. 10 - Процес підпису документу

Електронні підписи легко копіюються або підробляють, а також не передбачають механізм для перевірки або стандартизації. З іншого боку, цифрові підписи можуть бути використані для перевірки того, що конкретний

документ був дійсно підписаний певною особою. Цифровий підпис забезпечує спосіб видачі сертифікатів, дозволяючи особі:

- позначити документ штампом, який тільки вони можуть генерувати;
- переконатися, що документ не може бути підроблений після його підписання.

Для роботи цифрових підписів вони вимагають, щоб кожна особа, яка підписала документ, мала ідентифікаційний номер (відкритий ключ) та пов'язаний пароль (приватний ключ).

Цифровий підпис складається з чотирьох компонентів: а) хеш-функція SHA-256; б) відкритий ключ; в) приватний ключ; г) мітка часу зафіксована в момент видачі сертифіката.

Документ підписується шляхом об'єднання хешу документа з приватним ключем особи для створення нового унікального коду. Отриманий підпис потім об'єднано в документ разом з міткою часу.

Оскільки підпис є комбінацією цих двох компонентів, він:

- унікальний для цього конкретного документа, оскільки він був створений з хешу документа;
- може бути створено лише від особи, яка має приватний ключ. Слід зазначити, що оскільки підпис штамповано в цифровий документ, "підписаний" цифровий документ має інше значення хешу для непідписаного цифрового документа.

Навіть після підписання сертифікату, якщо змінити тільки одну букву документа, доведеться перерахувати хеш-функцію, яка не буде тотожною до попередньої. Крім того, підпис не можливо розшифрувати для отримання приватного ключа.

Якщо третя сторона бажає підтвердити цифровий підпис, вона повинна знати відкритий ключ особи, яка підписала документ. Оскільки

загальнодоступні ключі фактично є ідентифікаторами, вони, як правило розміщуються в загальних каталогах, подібних до телефонних книг.

Програмне забезпечення перевірки працює шляхом введення документа та відкритого ключа, а також перевіряє, що підпис у документі відповідає хешу оригіналу документа та що підпис документа математично пов'язаний з відкритим ключем особи, яка стверджує, що підписав документ зі своїм приватним ключем. Програма перевірки вміє це робити, не розкриваючи при цьому приватний ключ. Приклад такої архітектури зображений на рис. 11.

У відкритих інфраструктурах довірені органи, відомі як сертифікаційні органи, централізовано керують системою шляхом:

- видачі пов'язаних приватних і відкритих ключів;
- керуванням сервера для видачі часу кожного підпису;
- керуванням програми перевірки.

Зазвичай сертифікаційний орган додає відкритий ключ у сертифікат, який містить набір додаткових метаданих для полегшення використання. Це має декілька переваг:

- сертифікаційні органи можуть перевіряти осіб, яким видаються ключі, таким чином, прив'язуючи загальнодоступні ключі до ідентифікацій реального світу;
- кожен може довіряти даті підписання, оскільки часові штампи виставляються лише органом сертифікації.

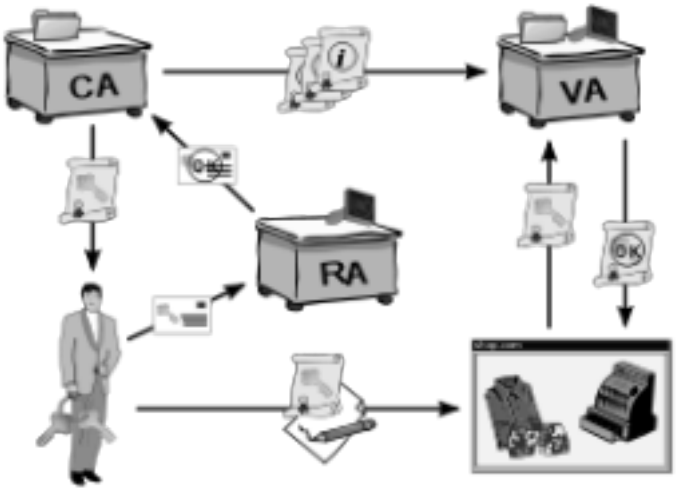


Рис. 11 - Інфраструктура відкритих ключів

Проте інфраструктура відкритих ключів також створює центральну точку контролю та відмов. Найбільш критичним є ситуація, коли сертифікаційному органу доводиться закривати програмне забезпечення для перевірки (скажімо, через банкрутство, громадянські заворушення, реструктуризацію тощо), це фактично призведе до того, що будь-який документ, підписаний ним, недійсний. Це створює серйозну проблему для отримання сертифікатів, таких як народження, одруження або освітні досягнення, які повинні тривати протягом усього життя. Крім того, орган сертифікації може зловживати довірою, розміщеною в них, будь-яким із способів. Інша особа може привласнити приватний ключ та видати фальшиві записи та контент на схожій платформі. Навіть якщо емітент публічно скасовує ці записи, незалежний верифікатор не буде знати різницю між дійсним та недійсним реквізитом, якщо не було деяких додаткових захисних механізмів, що підтверджують, коли відбулася транзакція та ким.

Технологія Blockchain підходить як нова інфраструктура для захисту, обміну та перевірки навчальних досягнень. У блокчейн PKI замінює центральну владу більш надійною децентралізованою мережею. Ця децентралізована структура підвищує довговічність мережі, оскільки дублікати блоків зберігаються у багатьох сторін. Децентралізація блокчейн дає йому додаткову

перевагу в тому, що жоден сторонній сервіс не може змінити або стерти транзакції, що зберігаються в блоках (рис. 12).

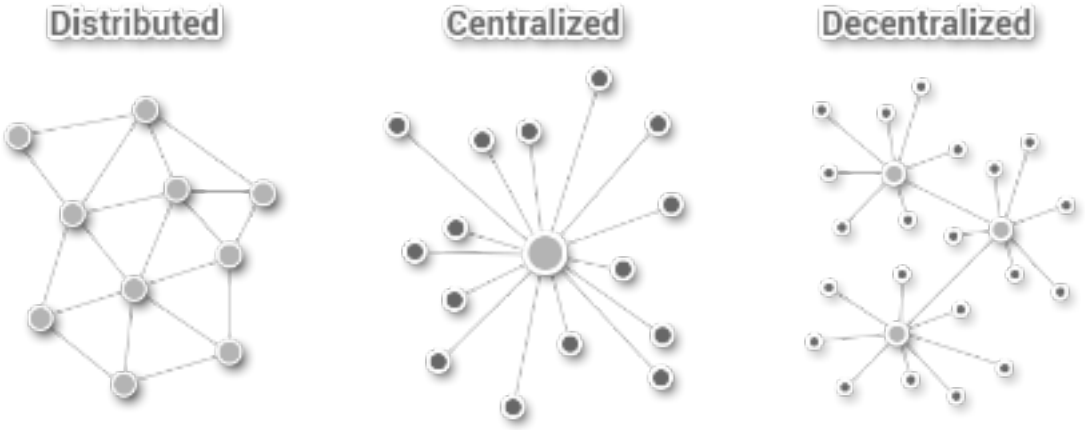


Рис. 12 - Приклад децентралізованої та розподіленої архітектур

Крім видалення залежності від будь-якого органу сертифікації або надійної сторонньої сторони, використання блокчейн забезпечує незалежне штампування часу, що створює значні переваги безпеки. Надійна позначка часу, безумовно, важлива у випадках, коли закінчується термін дії повноважень. Також має вирішальне значення з практичної точки зору, те що емітент повинен мати можливість змінювати ключі, що видаються, на регулярній основі для підвищення надійності всієї системи. Щоб визначити, що реквізити було випущено конкретним емітентом потрібно знати незалежну позначку часу та дійсний публічний ключ. На відміну від багатьох PKI-систем, підписи на блокчейні також не залежать від файлів, тому що програмне забезпечення можна використовувати для підписання будь-якого файлу, незалежно від стандартів, за допомогою яких цей файл був створений.

У випадку сертифікації блокчейн зберігає список емітента та одержувача кожного сертифіката разом із підписом документа (хеш) у відкритій базі даних, яка тотожно зберігається на тисячах комп'ютерів у всьому світі.

Самі цифрові облікові дані можуть бути збережені користувачем на жорсткому диску або в мобільному кошельнику, звідки їх легко можна

поділитися з іншими або навіть роздрукувати на папері. Таким чином, користувач може перевірити, хто видав сертифікат, хто його отримав, та перевірити вміст самого сертифікату.

Дані, необхідні для перевірки цілісності та автентичності сертифіката, зберігаються у блокчейні. Наприклад, для перевірки облікових даних роботодавець (або компанія, що надає послуги перевірки) суттєво дотримуватиметься вищезазначеного процесу, щоб переконатися, що хеш відповідає оригінальному файлу, а також, що ключі, що використовуються емітентом, належать до потрібної установи.

Якщо безконтактний, або загальнодоступний, блокчейн використовується для видачі або отримання сертифікатів, це означає, що кожен може використовувати блокчейн для забезпечення постійного доступу до підписів та механізму перевірки, якщо працює щонайменше одна копія бази даних. Верифікація відбувається шляхом зіставлення хеш документа, що перевіряється, з загальнодоступним хешем в блокчейні. Якщо вони співпадають, документ є справжнім. Це означає, що будь-хто, хто отримує сертифікат, який був підписаний на блокчейні, може перевірити його справжність.

Якщо використовується дозволений, або приватний (рис. 13), блокчейн, це означає, що лише люди, яким дозволено доступ до конкретної мережі блокчейнів, зможуть видавати, одержувати або перевіряти підписи на блокчейні.

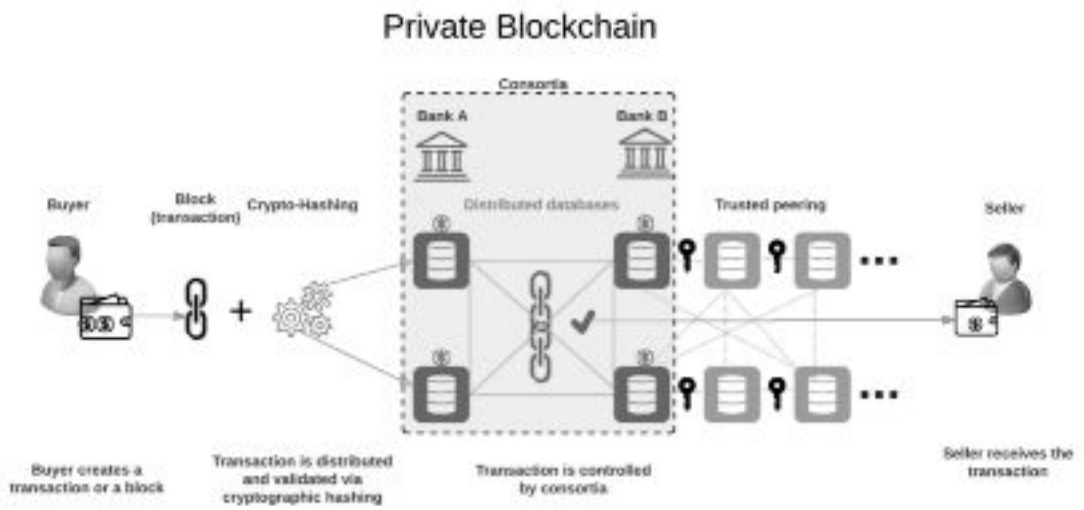


Рис. 13 - Приклад приватної мережі блокчейн

Цифрові документи можуть бути так само ефемерними, як і папір. Вони часто видаються у спеціальних форматах постачальниками для клієнтів, які без правильного програмного забезпечення неможливо зчитати або перевіряти їх. Навіть при доступі до правильного програмного забезпечення, у багатьох випадках процес підтвердження може бути довготривалим та ненадійним. Те саме стосується цифрових підписів, навіть в тих місцях, де законодавство передбачає їх прийняття, цифрові підписи входять у широкий діапазон форматів з різним рівнем безпеки, не всі з яких приймаються як юридичні докази.

Ще однією проблемою з цифровими документами є те, що один із основних способів, через який люди діляться інформацією в цифровій формі (електронна пошта), зазвичай не захищені, тому необхідно створювати приватні інфраструктури передачі для надсилання конфіденційних документів, таких як медичні записи. Це значно покращує безпеку поштових відправлень, але підвищує використання ресурсів для підтримання такої системи. Нарешті, як і паперові документи, цифрові документи також можуть бути підроблені досвідченими користувачами.

Коли технологія блокчейнів використовується при видачі сертифікатів, існує можливість не просто перевіряти облікові дані без посередника, а

збагатити та додавати новий функціонал до вже існуючої екосистеми цифрової сертифікації. BADGR та Mozilla Open Badge вже використовуються для забезпечення цифрових сертифікатів студентам у деяких престижних навчальних закладах.

Мета посвідчення в блокчейні полягає в тому, щоб перетворити цифровий сертифікат, який студент, як правило, отримує в приватному вигляді, в сертифікат, який автоматично перевіряється, та з якою треті сторони можуть звертатися за допомогою незмінної системи підтвердження у загальнодоступній блокчейн системі.

У сучасній практиці доступ до публічної платформи практично неминуче вимагає, щоб учень поділився чи розкривав свої метадані, що, як правило, включає в себе приватну інформацію. Використовуючи блокчейн як систему підтвердження навчальних досягнень, така приватна інформація не обов'язково повинна бути розголошена під час публічного пошуку по метаданим, що стосуються сертифікатів.

У короткостроковій перспективі цілком імовірно, що студенти зможуть підходити до академічних інститутів та роботодавців, зберігаючи при цьому стриманий рівень конфіденційності. Загалом, лише інформація, яку студенти позначатимуть як громадськість під час процесу створення доказів, будуть доступні третім особам. Додатки можуть дати можливості для програмних організацій, які можуть полегшити та спростити процес доступу до блокчейн для студентів та установ (інститутів, компаній, шкіл тощо). В ідеалі додатки будуть побудовані за допомогою відкритої архітектури, яка може гарантувати безперервність навчальних досягнень протягом усього життя та в усьому світі, а також відсутність блокування з одним конкретним рішенням.

Академічні інститути та компанії можуть скористатися перевагами підзвітності та узгодженості інформації, доступної на платформ блокчейн. Студенти, у свою чергу, можуть використовувати загальнодоступні метадані

для пошуку аналогічних профілів, і, таким чином, сприяти створенню нових моделей соціальної інтеграції та підприємництва. Усе це, не вимагаючи централізованого повноваження гарантувати дійсність інформації.

Висновок до розділу

У цьому розділі розглянуто блокчейн технологію, складові елементи цієї технології, такі як цифровий підпис, хешування, книги обліку. Також описано високорівневу та технічну частину розробки та розгортання блокчейн системи.

В останньому підрозділі визначено цифрові сертифікати за допомогою блокчейн технології. Визначено компоненти цифрового підпису, процес підписання документа за допомогою цифрового підпису, процес перевірки валідності сертифіката і цифрового підпису та сучасні інфраструктури, які керують сховищами публічних ключів і даних.

Як висновок сформулювано головну мету блокчейн технології при сертифікації даних, додану вартість цифрових сертифікатів, захищених блокчейн системою та цінність впровадження технології блокчейн в освіті.

РОЗДІЛ 3. ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ТА ЗАСТОСУВАННЯ РОЗРОБЛЮВАННОЇ СИСТЕМИ

3.1 Огляд архітектури системи

Система складається з чотирьох компонентів: верифікаційна програма, включаючи ідентифікацію користувачів, програма видачі сертифікатів для цифрових даних, яка передбачає відкликання з багатьма підписами та BTC-адресами, блокчейн та локальна база даних MongoDB. Контекстна діаграма архітектури системи зображена на рис. 14.

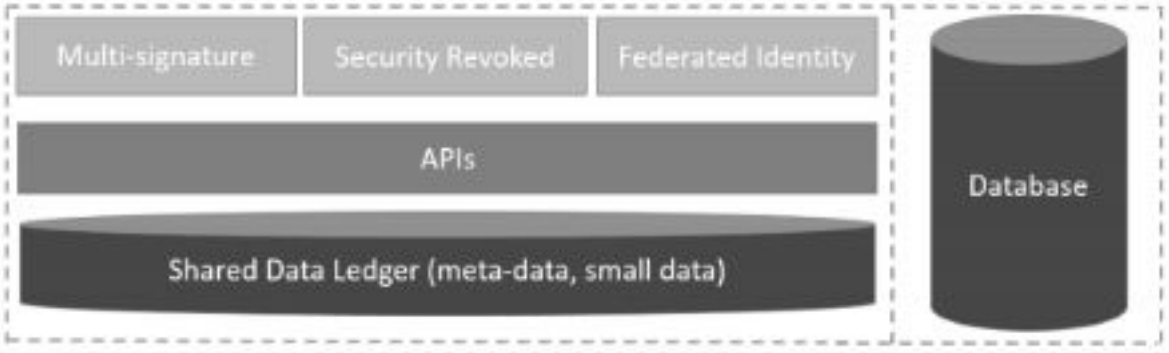


Рис. 14 - Контекстна діаграма архітектури системи

За основну бізнес-логіку системи відповідають додатки для сертифікатів та основними функціями такої системи є подання заявки, перевірка, підписання та видача сертифікату Такі програми призначені для об'єднання хеш-сертифіката в дереві Merkle і відправлення цього корня Merkle в блокчейн, після того як дані підписали більшість членів спільноти. Також програми включають можливість скасування сертифіката.

Програма підтвердження зосереджена на перевірці автентичності та цілісності виданих сертифікатів. Вона включає в себе два основних компоненти: веб-сторінка та додаток для різних платформ. Вони використовують один і той самий механізм і отримують транзакційне повідомлення через API та порівнюють повідомлення транзакції з даними підтвердження з квитанції. Механізм можна коротко описати наступним чином: перевірити правильність коду автентифікації; перевірити хеш із місцевим

сертифікатом; підтвердити хеш у дереві Merkle; забезпечити розміщення кореня Merkle в блоці; перевірити активність сертифікату; перевірити термін дії сертифіката. Також слід зазначити, що для зручності спільного використання сертифікатів програма дозволяє перевіряти документи, скануючи QR-код безпосередньо. Блокчейн виступає в ролі інфраструктури довіри та розподіленої бази даних для збереження даних автентифікації. Як правило, дані автентифікації складаються з кореня Merkle, створеного за допомогою хеш-даних з тисяч сертифікатів. MongoDB використовується як наша база даних, оскільки MongoDB успішно керує сертифікатами на базі JSON і забезпечує високу доступність та масштабованість. Також в якості системи керування базами даних можна використати PostgreSQL, яка має підтримку JsonField та в багатьох порівняльних тестах обходить по швидкодії нереляційні бази даних.

3.2 Огляд архітектури баз даних

База даних розроблена таким чином, щоб вона містила дві категорії даних: дані публічної автентифікації та приватні дані сертифікатів. Дані про загальну автентифікацію доступні для громадськості та записані в блокчейні. Дані приватного сертифіката зберігаються в MongoDB, де він надійно захищений та ізольований у внутрішній мережі.

На рис. 15 представлена діаграма потоку даних верхнього рівня.

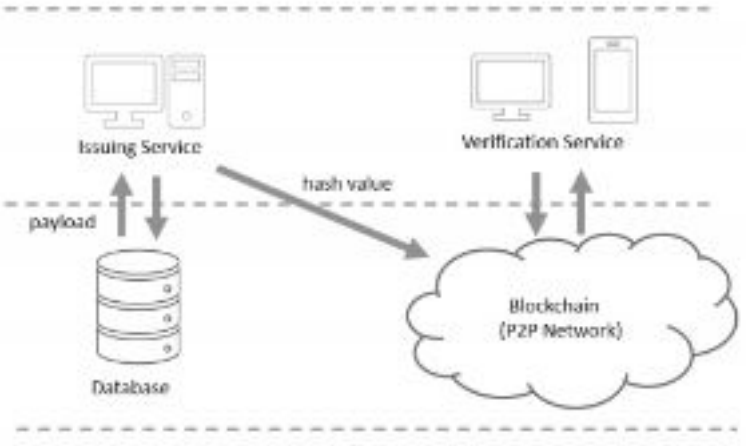


Рис. 12 - Архітектура бази даних

Це показує, що потік даних є однонаправленим від внутрішніх частин системи до мережі інтернет.

Система видачі зчитує сертифікат з MongoDB і транслює свої дані до блокчейна. Служба верифікації потребує доступу лише до блокчейн, щоб перевірити дійсність сертифіката.

У той же час, архітектура MongoDB підприємства прийнята як локальна база даних, як показано на рис. 16. У цій архітектурі "Mongo Server" служить як маршрутизатор для доступу до основної служби, "configure server" підтримує роботу системи метаданих та "монго-сервер" зберігає основні дані.

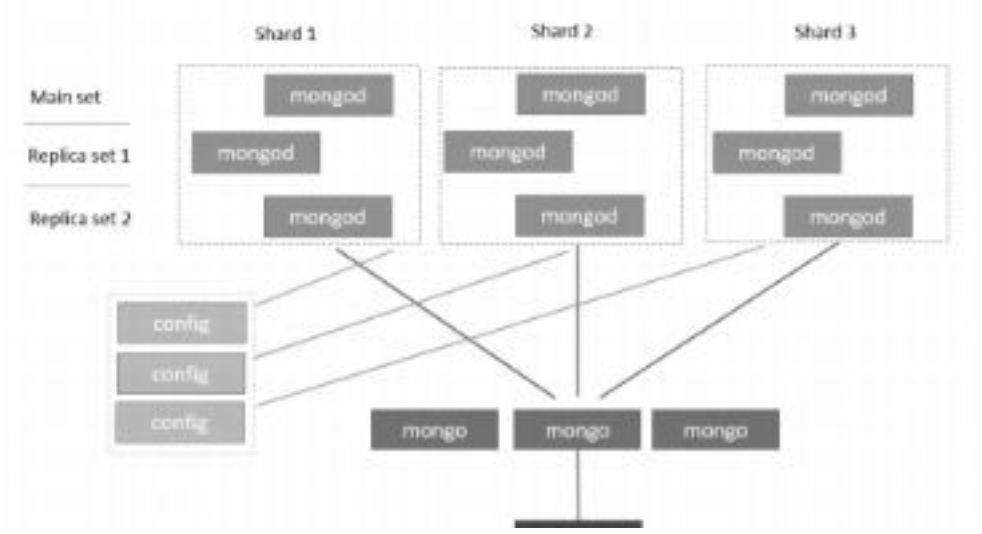


Рис. 16 - Кластераційна архітектура MongoDB.

3.3 Функції системи. Додатки верифікації

Програми верифікації відповідають за перевірку автентичності та цілісності сертифікатів, виданих раніше. В основному це два компоненти: веб-додаток та клієнтська програма. Програми верифікації отримують транзакцію та інформацію про підтвердження через API блокчейна, після чого система автентифікує перевірку підтвердження інформації, порівнюючи її з інформацією, яка зберігається в блокчейні.

Функції основних компонентів можна описати так:

- завантажити файли PDF / сканувати QR-коду;
- обчислити значення хеш-файлу у файлі PDF;

- клієнт робить запит до API блокчейна та дістає необхідну інформацію, якщо має доступ до цієї API;
- логіка верифікації:
    - управління автентифікацією: адреса електронної пошти навчального закладу чи установи;
    - верифікація хеш-значення на сертифікаті (щоб уникнути втручання);
    - перевірка, щоб підтвердити, чи є значення хеш-пам'яті в дереві merkle;
    - верифікація, щоб перевірити, чи є хеш-значення кореневого дерева merkle дерева на блоці;
    - перевірка дійсності сертифіката (щоб уникнути скасованого сертифіката);
    - перевірка дійсної дати сертифіката (щоб уникнути закінчення терміну дії сертифіката).

3.4 Функції системи. Додатки видачі сертифікатів

Додатки видачі сертифікатів несуть відповідальність за основну бізнес-логіку, яка включає в себе сертифікати, застосування, перегляд, перетворення та видачу. Додаток об'єднує хеш-сертифікати в дереві merkle і посилає корінь merkle до блокчейну за допомогою інтерфейсу API.

Функції основних компонентів можна описати так:

- функція входу:
    - захист входу;
    - скидання забутого пароля (опція);
- контроль прав:
    - ролі користувачів з різними правами доступу;
    - різні сторінки при зміні ролі користувача;

- процес схвалення (студент - перевірка - керівник - адміністративний персонал - керівник школи);
- багатофункціональний підпис сертифікату за допомогою використаних алгоритмів;
- ревізія сертифіката:
    - перегляд опублікованого сертифіката;
    - перегляд сертифікованого сертифіката;
    - перегляд сертифіката, готового до підписання;
- скасування сертифіката для одного сертифіката або для пакетних сертифікатів;
- переключення різних середовищ (середовище середовища виконання/середовище тестування);
- сторінка адміністрування для керування даними, правами та ін.

3.5 Прототип робочого циклу

Для реалізації вищезазначеного дизайну та аналізу створено модельний робочий процес прототипу для чотирьох основних ролей, включаючи студент, перевірку, емітент, систему та роботодавця. Робочий процес прототипу показаний на рис. 17.

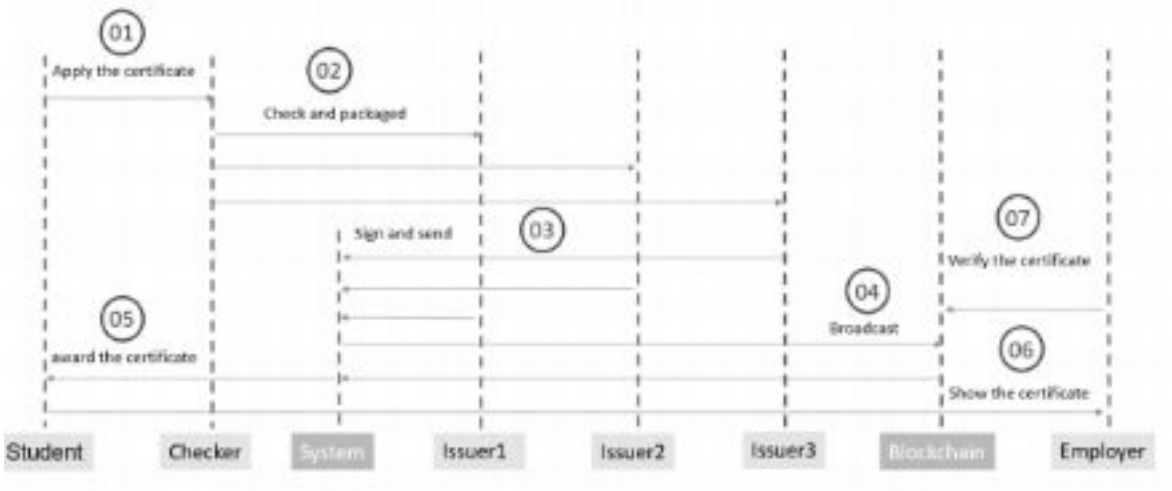


Рисунок 17. - Прототип робочого циклу

Зокрема робочий цикл прототипу полягає в наступному: по-перше, студент звертається до школи за отриманням підтвердження отриманих

навичок, знань, а сертифікатори перевіряють інформацію про студентів і об'єднують облікові дані за допомогою транзакції Bitcoin після його затвердження. Тоді більшість членів академічного комітету підписують його своїми приватними ключами. Після цього система передає транзакцію, яка містить корінь Merkle для всіх сертифікатів. Після виконання вищезазначеного кроку учень отримує сертифікат на основі JSON, коли операція підтверджена учасниками блокчейн системи. На наступному етапі студент надає роботодавцю сертифікат на основі JSON, коли він або вона подає заявку на роботу. Нарешті, компанія перевіряє сертифікат через доступ до блокчейн та перевіряє код автентифікації.

3.6 Розгортання системи

Для розгортання розроблюваної системи застосовується Docker, система для автоматизованого розгортання та керування додатками в середовищі віртуалізації на рівні операційної системи. В якості операційної системи використовується Ubuntu. Використання такої системи має такі переваги:

1) швидке розгортання додатків;

2) переносимість між різними машинами;

3) контроль версій та повторне використання компонентів;

4) спільне використання, використання віддаленого репозиторію;

5) легкі розміри та мінімальні накладні витрати;

6) спрощене обслуговування.

Основні можливості Docker: розміщення в ізольованому середовищі різнорідної конфігурації, різного роду додатків; використання контейнерів для ізоляції процесів; ізоляція на рівні файлової системи; ізоляція ресурсів для кожного окремого контейнера; ізоляція на рівні мережі; загальний лог для всіх контейнерів; використання інтерактивної командної оболонки; підтримка використання різних систем зберігання; використання готових образів для побудови створення контейнерів, що містять складні програмні стеки.

На першому етапі використання Docker потрібно написати файл для створення образу додатку. Такий файл називається Dockerfile, який є текстовим файлом зі списком команд, які Docker викликає під час створення образу. Це простий спосіб автоматизувати процес створення образу системи. Більшість команд для цього файлу ідентичні командам із операційної системи Linux. Тобто для того, щоб створити новий образ не потрібно знати додаткові команди окрім основних Linux команд для написання bash сценаріїв. За допомогою Dockerfile створюється образ нашого додатка, який потім запускається з різними контейнерами для синхронізованої роботи.

В якості проксі-сервера використовується Nginx. Для взаємодії між Python додатком, що виконується на стороні сервера, та самим веб-сервером використовується стандарт Web Server Gateway Interface Gunicorn. Основні можливості Gunicorn системи:

1. підримка більшості веб-фреймворків, зокрема Django;
2. автоматичне управління робочим процесом;
3. проста конфігурація python додатка;
4. можливості створення декількох конфігурацій для одного додатка;
5. можливість розширення функціональності за допомогою сторонніх утиліт;
6. сумісність з обома версіями python.

Для того, щоб використовувати декілька сервісів на різних контейнерах для Docker використовується інструмент Compose, який дозволяє за допомогою однієї команди створювати та запускати всі сервіси з файлу конфігурації. Для розроблюваного додатку потрібно створити контейнери для PostgresSQL, MongoDB, Nginx, Redis, Rabbitmq. Для конфігурації та запуску всіх сервісів разом з додатком використовується docker-compose файл.

Для створення образу додатка використовується команда

docker build –t product .

Файл з конфігурацією Docker має знаходитись в директорії, де запускається команда.

Для запуску всіх сервісів за допомогою Composer використовується команда docker-compose run.

3.7 Документація по проекту

Документація програмного забезпечення - супроводжуючі документи до програмного забезпечення, які містять в собі інформацію, що описує загальні положення необхідні для ознайомлення перед тим як використовувати його за призначенням. Така документація дуже важлива і описує не тільки яким чином правильно використовувати поставлене програмне забезпечення, а й пояснює основні використані алгоритми. В залежності від складності кожного окремого програмного забезпечення, його специфіки, а також ліцензії під якою воно створене - документація може варіюватися за обсягом і за змістом.

Для генерації документації використовується застосунок Sphinx. Sphinx – це генератор документації, який перетворює файли в форматі reStructuredText в HTML, (PDF, EPub і man). Використовує ряд розширень для reStructuredText (наприклад, для автоматичної генерації документації по вихідному коду, створення математичних формул або підсвічування вихідного коду). Широко використовується для документування програм мовою *Python*. З моменту виходу був прийнятий багатьма важливими Python-проектами.

Висновок до розділу

У даному розділі описано архітектури системи, головні функції основних додатків, процес розгортання додатку за допомогою Docker системи та описано процес створення взаємодії і запуску всіх сервісів в різних контейнерах, які використовуються додатком. Були вказані переваги використання Docker системи. Також побудовано документацію за допомогою бібліотеки Sphinx, яка використовує автогенерування, використовуючи коментарі до класів, полів та модулів.

РОЗДІЛ 4. РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

Розроблення та виведення стартап-проекту на ринок передбачає здійснення низки кроків, в межах яких визначають ринкові перспективи проекту, графік та принципи організації виробництва, фінансовий аналіз та аналіз ризиків і заходи з просування пропозиції для інвесторів. Узагальнено етапи розроблення стартап-проекту можна подати таким чином:

1) маркетинговий аналіз стартап-проекту - розробляється опис самої ідеї проекту та визначаються загальні напрями використання потенційного товару чи послуги, а також їх відмінність від конкурентів;
2) організація стартап-проекту - визначається плановий обсяг виробництва потенційного товару, на основі чого формулюється потреба у матеріальних ресурсах та персоналі; розраховуються загальні початкові витрати на запуск проекту та планові загальногосподарські витрати, необхідні для реалізації проекту.
3) фінансово-економічний аналіз та оцінка ризиків проекту - розраховуються основні фінансово-економічні показники проекту (обсяг виробництва продукції, собівартість виробництва, ціна реалізації, податкове навантаження та чистий прибуток) та визначаються показники інвестиційної привабливості проекту (запас фінансової міцності, рентабельність продажів та інвестицій, період окупності проекту);
4) заходи з комерціалізації проекту - цей етап спрямовано на пошук інвесторів та просування інвестиційної пропозиції (оферти).

4.1 Опис ідеї проекту

Однією з основних причин створення, успішного розвитку та подальшого існування стартапів вважають неповороткість і повільність великих корпорацій, які успішно використовують уже наявні продукти, а розробкою і створенням нових майже не займаються. Децентралізовані платформи швидко показали користувачам мережі, що вони допомагають економити час і фінансові ресурси,

домагаючись кращих результатів в порівнянні з традиційними підходами. Тому стартапи, завдяки своїй мобільності в плані втілення нових ідей становлять конкуренцію великим корпораціями.

Основним ресурсом для створення нового стартапу служить хороша новаторська ідея. Власне за свіжими і незвичайними ідеями женуться багато і часто купуючи їх не шкодують великі суми. Сама ідея, яка не має ніякого матеріального втілення, а існує тільки на папері або на словах (план стартапу), може коштувати дуже багато. Іншим фактором успішності цієї ідеї є її затребуваність (ступінь необхідності для споживача), адже ідея може бути незвичайної і новою, але користі від неї буде мінімум.

Стартапи покликані вирішувати проблеми і завдання, які з часом стає можливим вирішити завдяки використанню результатів технічного прогресу. Або, як казав засновник Twitter'a Ісаак "Біз" Стоун, сучасні високотехнологічні проекти повинні служити одній меті: спрощувати користувачам будь-які дії в їх повсякденному житті.

Зміст ідеї розроблюваного стартапу - це платформа сертифікації веб-сайтів із цифровим процесом сертифікації, що базується на технології блокчейн для захисту автентифікації сертифікатів, зберігання даних та запобігання підробкам сертифікатів. Це екосистема для всіх учасників ринку сертифікації. Для бізнесу система відповідає основним вимогам сертифікації. Система включає в себе такі критерії, як - ціна, близькість до вашого місцезнаходження, рейтинг і репутація органу, а також опис всіх стадій сертифікації, що робить процедуру простими та зрозумілими. Всі дії учасників сертифікації та сертифікати зберігаються в блокчейні, тому ви можете бути повністю впевнені в їх надійності та прозорості всіх процедур.

В межах підпункту було проаналізовано і подано у вигляді таблиці 4.1:

- зміст ідеї (що пропонується);
- можливі напрямки застосування;

- основні вигоди, що може отримати користувач товару (за кожним напрямком застосування);
- чим відрізняється від існуючих аналогів та замінників.

Таблиця 4.1 – Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигоди для користувача
Система сертифікації даних за допомогою блокчейн технології для автентифікації, підпису даних та зберігання сертифікатів	сертифікація навчальних досягнень	підвищення довіри до навичок освітянина; підвищення надійності зберігання сертифікатів та інформації про досягнення певних навичок
	сертифікація акредитації установ	видача акредитації для різних установ дозволить підвищити швидкість перевірки певного органу, його повноважень, що підвищує довіру до такої установи
	використання паспорту навчання	дозволить користувачам зберігати всі свої навчальні досягнення в одному кабінеті користувача, що дозволить швидко отримувати інформації при навички для сторонніх систем, яким користувач предоставив доступ
	ідентифікація освітян навчального закладу	дозволяє ідентифікувати освітян певного навчального закладу, створення надійного реєстру даних студентів закладу з використанням паспорту навчання

Аналіз потенційних техніко-економічних переваг ідеї (чим відрізняється від існуючих аналогів та замінників) порівняно із пропозиціями конкурентів передбачає:

- визначення переліку техніко-економічних властивостей та характеристик ідеї;
- визначення попереднього кола конкурентів (проектів-конкурентів) або товарів-замінників чи товарів-аналогів, що вже існують на ринку, та проведення збір інформації щодо значень техніко-економічних показників для ідеї власного проекту та проектів-60 конкурентів відповідно до визначеного вище переліку;
- проведення порівняльного аналізу показників: для власної ідеї визначені показники, що мають а) гірші значення (W, слабкі); б) аналогічні (N, нейтральні) значення; в) кращі значення (S, сильні) (таблиця 4.2).

Таблиця 4.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

№	Техніко-економічні характеристики ідеї	(потенційні) товари/концепції конкурентів	W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
1	Собівартість	Система сертифікації даних на основі блокчейн	+		
2	Зручність використання			+	
3	Надійність				+
4	Швидкість обробки транзакцій, отримання інформації				+
5	Доступність				+

Визначений перелік слабких, сильних та нейтральних характеристик та властивостей ідеї потенційного товару є підґрунтям для формування його конкурентоспроможності.

4.2 Технологічний аудит ідеї проекту

Визначення технологічної здійсненності ідеї проекту передбачає аналіз таких складових (таблиця 4.3):

- за якою технологією буде виготовлено товар згідно ідеї проекту?
- чи існують такі технології, чи їх потрібно розробити/доробити?
- чи доступні такі технології авторам проекту?

Таблиця 4.3 – Технологічна здійсненність ідеї проекту

Ідея проекту	Технології її реалізації	Наявність технології	Доступність технологій
використання блокчейн	блокчейн мережа	є в наявності	доступно в різних конфігураціях
використання смарт контрактів	смарт контракти Ethereum	є в наявності	доступно
сертифікація даних за допомогою цифрового підпису	алгоритм цифрового підпису	є в наявності	має реалізацію на багатьох мовах програмування, відкритий, задокументований стандарт

Обрана технологія реалізації ідеї проекту: реалізація проекту можлива з використанням блокчейн технологій смарт-контрактів та цифровим підписом.

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Аналіз попиту показує, що використання сучасної системи сертифікації є привабливою для входження на ринок. Динаміка ринку використання, сертифікування даних зростає, все більше освітян отримують навички онлайн, які потребують належної сертифікації.

Після аналізу попиту визначено потенційні групи клієнтів, їх характеристики, та сформовано орієнтовний перелік вимог до системи для кожної групи (таблиця 4.4).

Таблиця 4.4 - Характеристика потенційних клієнтів стартап-проекту

№	Потреба, що формує ринок	Цільова аудиторія (цільові сегменти ринку)	Відмінності у поведінці різних потенційних цільових груп клієнтів	Вимоги споживачів до товару
1	сертифікація даних	органи, що потребують видачі сертифікованих даних	різні дані	надійність швидкість безпечність
2	акредитація організацій	органи, що потребують акредитації	акредитація в різних сферах дії, ринку	швидкий спосіб акредитації та підтвердження справжності інформації
3	зменшити час перевірки сертифікатів	студенти, науковці, навчальні установи, корпорації, установи пошуку робітників з відповідними навичками	використання сертифікатів для різних цілей	економічні вимоги швидкодія
4	зберігання сертифікатів	студенти, науковці, навчальні установи, корпорації, установи пошуку робітників з відповідними навичками	формування банків сертифікатів	надійність швидкодія доступу до банків інформації

Після визначення потенційних груп клієнтів було проведено аналіз ринкового середовища: складено таблиці факторів, що сприяють ринковому впровадженню проекту, та факторів, що йому перешкоджають (таблиці 4.5, 4.6). Фактори в таблиці подаються в порядку зменшення значущості.

Таблиця 4.5 – Фактори загроз

№	Фактор	Зміст загрози	Можлива реакція компанії
	Конкуренція	Поява більш швидкої та надійної системи сертифікації	Передбачити додаткові переваги власного проекту для того, щоб повідомити про них саме після виходу міжнародної компанії на ринок
	Економічний	Подорожчання проведення однієї транзакції	Оптимізація програмного продукту

Таблиця 4.6 – Фактори можливостей

№	Фактор	Зміст можливості	Можлива реакція компанії
	Науково-технічний	Покращення і оптимізація алгоритмів сертифікації даних	Адаптація існуючого рішення і алгоритмів під нову технологію
	Попит	Більш широке розповсюдження цифрових сертифікатів	Постійна підтримка продукту

Надалі було проведено аналіз пропозиції: визначили загальні риси конкуренції на ринку (таблиця 4.7).

Таблиця 4.7 – Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)
1. Вказати тип конкуренції: монополістична конкуренція.	Існує декілька фірм-конкурентів.	Підтримка якості продукту та постійні нововведення.
2. За рівнем конкурентної боротьби: міжнародний.	Фірми-конкуренти знаходяться в інших країнах.	Адаптація продукту як для вітчизняних так і для зарубіжних клієнтів.

Продовження таблиці 4.7 - Ступеневий аналіз конкуренції на ринку

3. За галузевою ознакою: міжгалузева.	Продукт використовується в різних галузях.	Постійне вдосконалення продукту та пошук нових ідей
4. Конкуренція за видами товарів: товарно-видова.	Види товарів однакові.	Створити продукт, враховуючи сильні і слабкі сторони конкурентів.
5. За характером конкурентних переваг: неціновa.	Вдосконалення технології сертифікації даних.	Зниження ціни на продукт та підтримка його якості.
6. За інтенсивністю: марочна.	Бренди існують і конкурують.	PR, реклама, просування бренду.

Було проведено аналіз конкуренції у галузі за моделлю М. Портера (таблиця 4.8).

Таблиця 4.8 - Аналіз конкуренції в галузі за М. Портером

	Прямі конкуренти в галузі	Потенційні конкуренти	Постачальники	Клієнти	Товари-замінники
Складові аналізу	CertBot, CertChain, BlockCerts	наявність вже існуючих рішень	органи акредитації	контроль якості продукту	поява уніфікованого та надійного методу сертифікації даних
Висновки:	доволі інтенсивна конкурентна боротьба з вже закріпившимися на ринку гравцями	є можливості виходу на ринок	можливість використовувати звичайні органи акредитації	клієнти диктують усі умови роботи на ринку	перехід усіх додатків для сертифікації даних на уніфіковани

					й метод

За результатами аналізу таблиці 4.8 було зроблено висновок про можливість роботи на ринку з огляду на конкурентну ситуацію. Також було зроблено висновок щодо характеристик, які повинен мати проект, щоб бути конкурентноспроможним на ринку. Цей висновок був врахований при формулюванні переліку факторів конкурентноспроможності у наступному пункті.

На основі аналізу конкуренції, проведеного в таблиці 4.8, а також із урахуванням характеристик ідеї проекту (таблиця 4.1), вимог споживачів до товару (таблиця 4.4) та факторів маркетингового середовища (таблиці 4.5, 4.6) визначається та обґрунтовується перелік факторів конкурентоспроможності. Аналіз оформлюється за таблицею 4.9.

Таблиця 4.9 – Обґрунтування факторів конкурентоспроможності

№	Фактор конкурентоспроможності	обгрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)
1	Виконання програмного забезпечення у кросплатформеному вигляді	Можливість використання програмного забезпечення на будь-якій платформі.
2	Надійність	Підвищення надійності сертифікації та верифікації даних
3	Довіра	Підвищення довіри до органів сертифікації та виданих сертифікатів

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін.

Таблиця 4.10 - SWOT- аналіз стартап-проекту

Сильні сторони: надійність, криптостійкість, швидкість, прозорість, доступність	Слабкі сторони: дороговизна, складність розгортання
Можливості: більш широке розповсюдження технологій з конкурентами, підтримкою системи сертифікації, поява нових технологій для підвищення надійності.	Загрози: видавлення з ринку, зміна потреб користувачів, поява нової системи

На основі SWOT-аналізу було розроблено альтернативи ринкової поведінки (перелік заходів) для виведення стартап-проекту на ринок та орієнтовний оптимальний час їх ринкової реалізації з огляду на потенційні проекти конкурентів, що можуть бути виведені на ринок (див. таблицю 4.8, аналіз потенційних конкурентів).

4.4 Розроблення ринкової стратегії проекту

Аналіз ринку являє собою кількісну і якісну оцінку ринку. Він дивиться на розмір ринку як за обсягом, так і у вартості, різні сегменти споживачів і купівельну поведінку, конкуренція і економічне середовище з точкою зору бар'єрів для входу та регулювання.

Для оцінки активності на ринку конкуруючих фірм, використовуються наступні показники: обсяг продажів продукції, частка в загальному обсязі продажів, характер продукції (технічні характеристики, ціна, новизна, доступність послуг), практика рекламних заходів; Практика звернення товарів (наявність складів, види транспорту, робота з дилерами і дистриб'юторами), маркетинговою діяльністю фірми (асортиментної політикою, напрямками для розробки нових продуктів, маркетингова політики, методи інтенсифікації продажів, цінової політики і тенденцій) рівень витрат виробництва і способи їх

зниження, фінансове становище, кількісні показники ефективності (продукції, інвестицій, наукових досліджень, використання виробничих потужностей й для виробництва конкуруючих продуктів).

Для аналізу потенційних покупців використовуються такі показники: становище на ринку, частка в загальному обсязі споживання товарів, основних постачальників продукції, твердих вимог до продукції, організаційної структури, торгових можливостей, методів роздрібної торгівлі, умови надання пільг покупцям і постачальники, ефективність каналів продажів, загальний обсяг продажів, рентабельність торгових операцій, сума витрат по реалізації, витрати на утримання складів, кількість комісій, отриманих фірмою за посередництво.

Аналіз роздрібних і оптових ринків. Роздрібний торговець або споживчий ринок покупців ринку товарів і послуг для особистого споживання. Процес загального дослідження роздрібного ринку повинен включати в себе визначення самого ринку (в першу чергу, товари і покупці цих товарів, які відрізняються доходами і споживанням, соціальний статус, національність, культурні традиції) і фактори, що визначають поведінку покупця при здійсненні покупки (економічні, науково-технічні, політичні, чинники культурного середовища). Процес, за допомогою якого покупець приймає рішення про покупку продукту полягає в розумінні необхідності продукту, пошук інформації про продукт, вибравши прийнятний варіант покупки, вибираючи покупки і реагування на покупку.

Знання характеристик роздрібного ринку і факторів, що визначають поведінку покупця дає можливість впливати на прийняття покупця про прийняття рішення про покупку товарів і визначити кількість майбутніх продажів продукції проекту.

Розроблення ринкової стратегії першим кроком передбачає визначення стратегії охоплення ринку: було проведено опис цільових груп потенційних споживачів (таблиця 4.11).

Таблиця 4.11 – Вибір цільових груп потенційних споживачів

№	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи (сегменту)	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
	Навчальні заклади	висока	високий	невисока	середня
	Роботодавці	висока	високий	висока	середня

За результатами аналізу потенційних груп споживачів було обрано цільову групу, для якої буде запропоновано даний товар, та визначено охоплення ринку - стратегію концентрованого стратегію маркетингу(компанія зосереджується на одному сегменті).

Для роботи в обраних сегментах ринку сформовано базову стратегію розвитку (таблиця 4.12).

Таблиця 4.12 – Визначення базової стратегії розвитку

№	Обрана альтернатива розвитку проекту	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції відповідно до обраної альтернативи	Базова стратегія розвитку
	Розробка програмного продукту, PR, просування бренду	Масовий маркетинг	Метод сертифікації даних за допомогою блокчейн технології	Стратегія диференціації

Наступним кроком обрано стратегію конкурентної поведінки (таблиця 4.13).

Таблиця 4.13 – Визначення базової стратегії конкурент

№	Чи є проект першопрохідцем на ринку?	Чи буде компанія шукати нових клієнтів, або забирати існуючих у конкурентів?	Чи буде компанія копіювати основні характеристики товару конкурента, і які?	Стратегія конкурентної поведінки
	Ні	Забирати існуючих	Ні	Стратегія наслідування лідеру

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту (див. таблицю 4.5), а також в залежності від обраної базової стратегії розвитку (таблиця 4.12) та стратегії конкурентної поведінки (таблиця 4.13) розроблено стратегію позиціонування (таблиця 4.14), що полягає у формуванні ринкової позиції (комплексу асоціацій), за яким споживачі мають ідентифікувати торговельну марку/проект.

Таблиця 4.14 – Визначення стратегії позиціонування

№	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту (три ключових)
	невисока плата за проведення транзакцій	позиціювання за показниками надійності	Відсутність подібних алгоритмів	Надійність, довіра, швидкість

Результатом виконання підрозділу стала узгоджена система рішень щодо ринкової поведінки стартап-компанії, яка визначає напрями роботи стартап-компанії на ринку.

4.5 Розроблення маркетингової програми стартап-проекту

Ефективний маркетинг починається з розглянутою, добре обізнаною маркетинговою стратегією. Хороша стратегія допоможе визначити бачення, місії та бізнес-цілі, а також описуються кроки, які необхідно зробити для досягнення цих цілей.

Стратегія впливає на спосіб запуск, тому вона повинна плануватися і розроблятися в консультації з вашою командою. Це широке охоплення і всеосяжний інструмент стратегічного планування, який:

- описує бізнес, продукти і послуги
- пояснює позицію і роль товарів і послуг на ринку
- профілі ваших клієнтів і ваших конкурентів
- визначає маркетингову тактику буде використовуватись
- дозволяє будувати маркетинговий план і оцінити його ефективність.

Маркетингова стратегія визначає загальний напрямок і цілі вашого маркетингу, і, отже, відрізняється від плану маркетингу, в якому викладаються конкретні дії, які необхідно виконати для реалізації маркетингової стратегії. Ваша маркетингова стратегія може бути розроблена протягом наступних декількох років, в той час як ваш маркетинговий план зазвичай описує тактику повинні бути досягнуті в поточному році.

Результатом підрозділу стала ринкова (маркетингова) програма, що включає в себе концепції товару, збуту, просування та попередній аналіз можливостей ціноутворення, спирається на цінності та потреби потенційних клієнтів, конкурентні переваги ідеї, стан та динаміку ринкового середовища, в

межах якого впроваджено проект, та відповідну обрану альтернативу ринкової поведінки.

Сформовано маркетингову концепцію товару, який отримує споживач. Для цього у таблиці 4.15 підсумовано результати попереднього аналізу конкурентоспроможності товару.

Таблиця 4.15 – Визначення ключових переваг концепції потенційного товару

№	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)
	Швидкість підтвердження	Використання книги обліку для швидкого пошуку даних	Рішення є швидким
	Надійність	Використання транзакції та цифрового підпису для підвищення надійності	Користувачу не потрібно піклуватися про безпечність використання системи

Останньою складової маркетингової програми є розроблення концепції маркетингових комунікацій, що спирається на попередньо обрану основу для позиціонування, визначену специфіку поведінки клієнтів (таблиця 4.16).

Таблиця 4.16 – Концепція маркетингових комунікацій

№	Специфіка поведінки цільових клієнтів	Канали комунікацій, якими користуються цільові клієнти	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення	Концепція рекламного звернення
	Клієнти обиратимуть зручніший	Соціальні мережі, електронна пошта,	Швидкодія, надійність, простота використан	Показати переваги продукту, швидкодію	Демо ролик з використанням, реклама

	товар з потрібними функціями.	мобільні телефони	ня, кросплатформеність		

Результатом підрозділу стала ринкова (маркетингова) програма, що включає в себе концепції товару, збуту, просування та попередній аналіз можливостей ціноутворення, спирається на цінності та потреби потенційних клієнтів, конкурентні переваги ідеї, стан та динаміку ринкового середовища, в межах якого впроваджено проект, та відповідну обрану альтернативу ринкової поведінки.

4.6 Висновки до розділу

В даному розділі було проведено аналіз програмного продукту у якості стартап проекту. Можна зазначити що у проекту є можливість комерціалізації, оскільки ринок технологій віртуальної реальності динамічно розвивається, створюються нові додатки із соціальною складовою, для яких потрібна можливість взаємодії з іншими користувачами.

Можна сказати, що подальший розвиток проекту є доцільним, оскільки він знайде свою цільову аудиторію. Для впровадження ринкової реалізації проекту слід обрати альтернативу, яка передбачає розробку програмного продукту.

ВИСНОВКИ

В магістерській дисертації розглянуто процес створення, впровадження та документування системи сертифікації даних за допомогою блокчейн технології.

Технологія блокчейн підходить як нова інфраструктура для захисту, обміну та перевірки навчальних досягнень. У випадку сертифікації блокчейн може зберігати список емітента та одержувача кожного сертифікату разом із підписом документа у відкритій базі даних, яка ідентично зберігається на тисячах комп'ютерів у всьому світі. Цифрові сертифікати, які, таким чином, захищені, мають значні переваги перед "звичайними" цифровими сертифікатами, у тому числі: вони не можуть бути підроблені - можна з точністю підтвердити, що сертифікат був спочатку виданий та отриманий тими самими особами, які вказані в сертифікаті; перевірка сертифіката може виконуватися програмним забезпеченням з відкритим кодом будь-ким, хто має доступ до блокчейну; відсутність необхідності для будь-яких посередників. Також механізм такого цифрового сертифікату дозволяє підписувати документ для публікації, не вимагаючи публікувати сам документ, таким чином зберігаючи конфіденційність документів.

У даній роботі проведено аналіз існуючих методів сертифікації даних, визначено основні недоліки та вимоги, які необхідні для сучасної системи сертифікації. Також розглянуто основи блокчейн технології. У другому розділі розглянуто блокчейн технологію, складові елементи цієї технології, такі як цифровий підпис, хешування, книги обліку та цифрові сертифікати за допомогою блокчейн технології. Підсумовано основну цінність блокчейн технології при сертифікації даних. В останньому розділі розроблено бізнес стратегії для запуску додатку на ринок, побудовано бізнес-план розвитку та впровадження нового рішення у існуючий ринок з великою кількістю конкурентів.

Таким чином, технологія блокчейн дає можливість створити надійну, безпечну та довірчу систему, яка працюватиме без посередників при видачі та підтвердженні освітніх досягнень. Технологія блокчейн вирішує основу проблему захисту від підроблення сертифікатів та інших освітніх досягнень.

Система сертифікації загалом може використовуватися для зберігання та верифікації даних в різних галузях суспільства. Наприклад, технологія блокчейн вже довела свою корисність в сфері банківських послуг. Платформа обміну повідомленнями SWIFT використовується фінансовими інститутами повсюдно для передачі інформації по транзакціях за допомогою стандартизованої системи кодів. Стійкість системи, в поєднанні з постійними оновленнями, дозволили їй стати лідером в області обробки міжбанківських платежів. Однак, через бюрократію банківської системи обробка деяких транзакцій займає години або навіть дні. Тому для скорочення часу транзакцій, підвищення надійності записів про транзакції можливо використовувати блокчейн технологію.

ПЕРЕЛІК ПОСИЛАНЬ

1. Blockcert Introduction [Електронний документ]. - 2018. - Режим доступу до ресурсу: https://www.blockcerts.org/guide/
2. Blockchain Technology [Електронний документ]. - 2017. - Режим доступу до ресурсу: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
3. Academic certificate [Електронний документ] - 2018. - Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Academic_certificate
4. Bitcoin and Blockchain: Trending in Finance Essay [Електронний документ]. - 2017. - Режим доступу до ресурсу: https://www.linkedin.com/pulse/bitcoin-blockchain-trending-finance-esssay-philip-capriglione/
5. A Survey on Security and Privacy Issues of Bitcoin [Електронний документ]. - 2017. - Режим доступу до ресурсу: https://arxiv.org/pdf/1706.00
6. Response to Blockchain & Blockcerts Critiques from Privacy Researcher [Електронний документ]. - 2017. - Режим доступу до ресурсу: https://community.blockcerts.org/t/response-to-blockchain-blockcerts-critiques-from-privacy-researcher/308
7. Towards Self-Sovereign Identity using Blockchain Technology [Електронний документ]. - 2017. - Режим доступу до ресурсу: https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf
8. «Architectural Styles and the Design of Network-based Software Architectures» [Електронний ресурс]. - Roy Thomas Fielding, 2000 – Режим доступу: http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm.
9. «Representional State Transfer (REST)». Бібліотека університету Каліфорнії. Бібліотека університету Каліфорнії [Електронний ресурс]. – Режим доступу: http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch

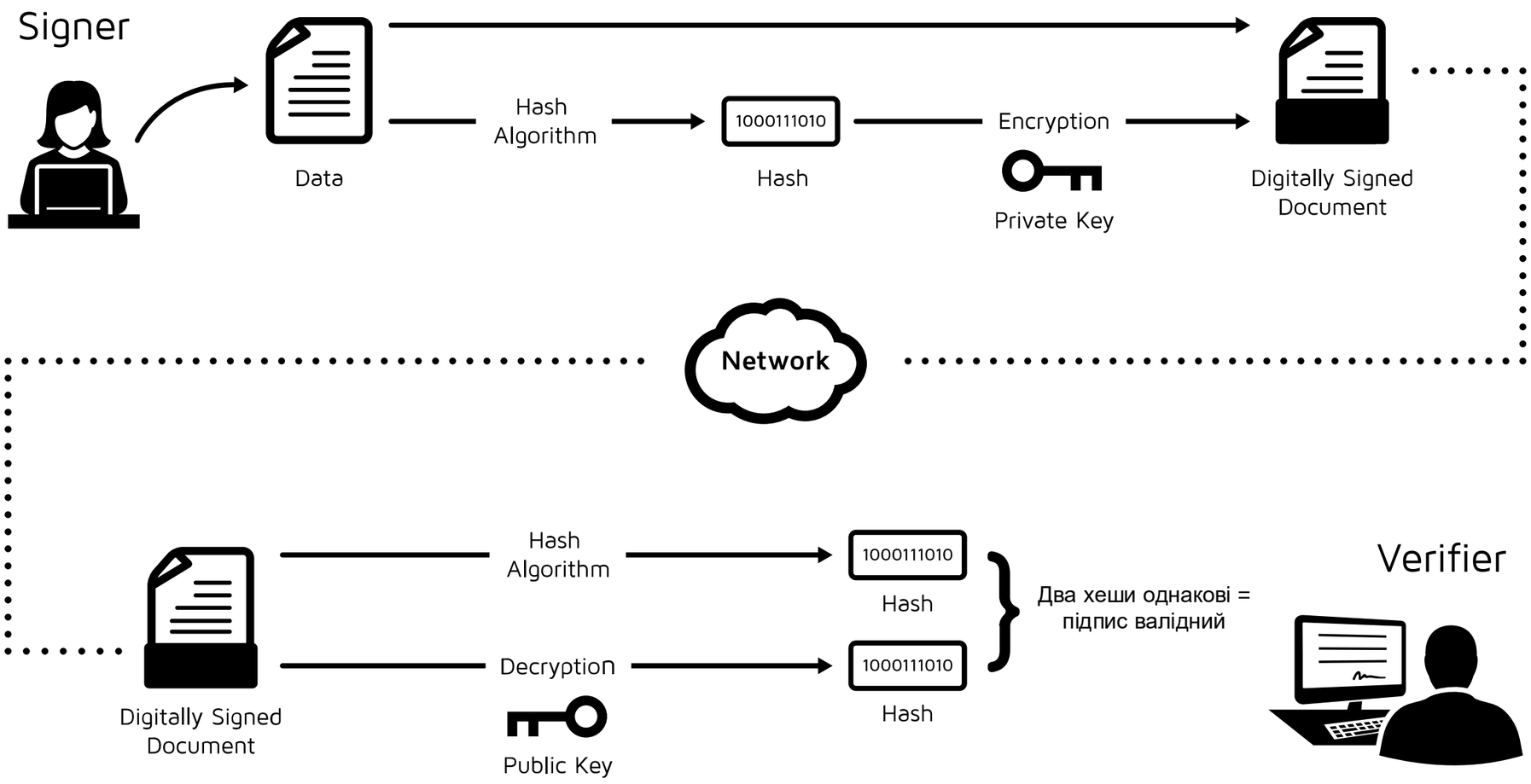
10. Public, Private and Consortium Blockchains: What's Right For You? [Електроний ресурс]. - 2018. - Режим доступу до ресурсу: https://www.draglet.com/blockchain-services/blockchain-technology/private-or-public-blockchain/
11. Blockchain: Foundational Technology To Change The World. Khudnev, Evgenii [Електроний ресурс]. - 2017. - Режим доступу до ресурсу: https://www.theseus.fi/bitstream/handle/10024/138043/Evgenii_Khudnev_Thesis.pdf?sequence=1
12. Design, Implementation, and Evaluation of a Blockchain-enabled Multi-Energy Transaction System for District Energy Systems. Yu, Qianchen [Електроний ресурс]. - 2018. - Режим доступу: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/25736/MasterThesis_QianchenYU_converted.pdf?sequence=4&isAllowed=y
13. The blockchain technology and its applications in the financial sector. Laura Jutila [Електроний ресурс]. - 2017. - Режим доступу до ресурсу: https://aaltodoc.aalto.fi/bitstream/handle/123456789/27209/bachelor_Jutila_Laura_2017.pdf?sequence=1

ДОДАТКИ

ДОДАТОК А

Процес підпису документа

Процес підпису документа



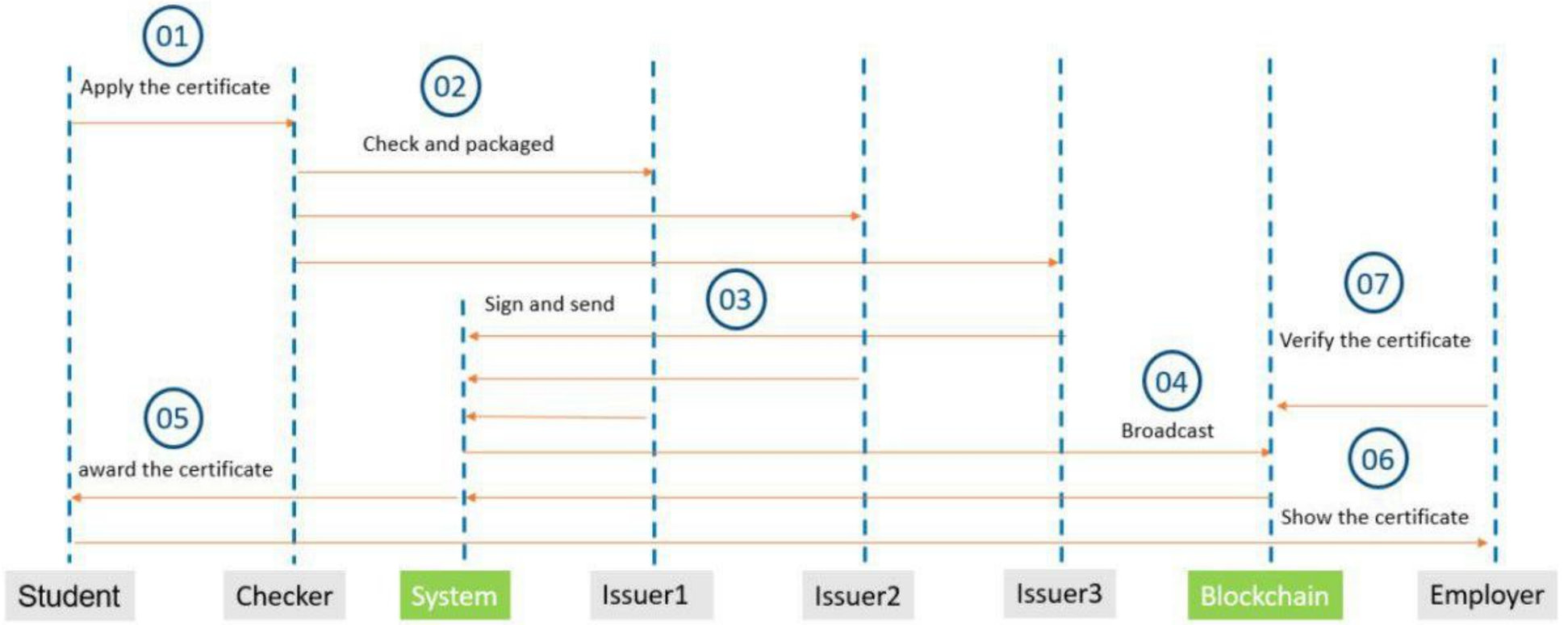
Демонстраційний плакат № 1
до магістерської дисертації на тему
„Система сертифікації даних на основі блокчейн технології”

Розробив: Осін О. Д.
Прийняв: Бурлаков В. М.

ДОДАТОК Б

Діаграма послідовності

Діаграма послідовності



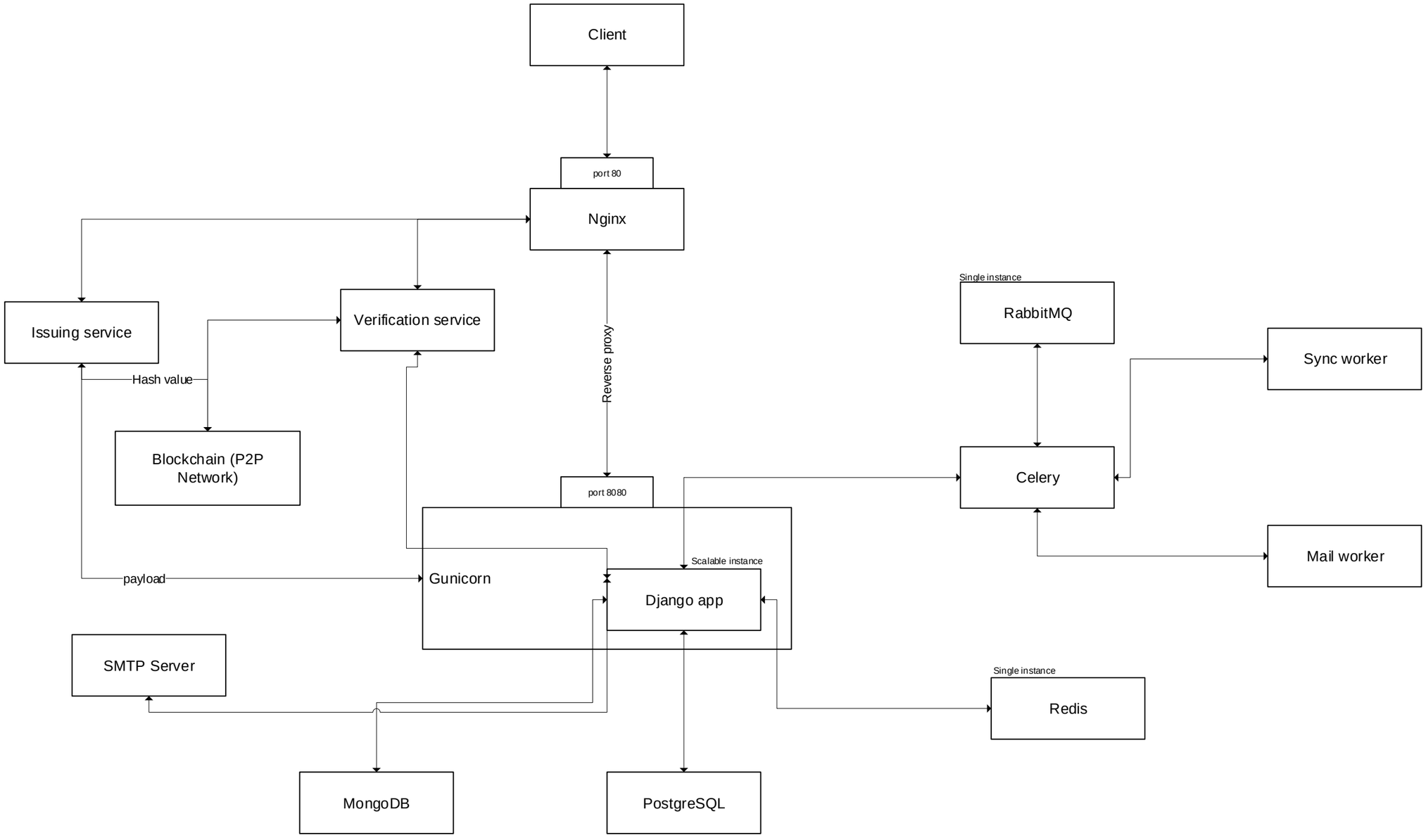
Демонстраційний плакат № 2
до магістерської дисертації на тему
„Система сертифікації даних на основі блокчейн технології”

Розробив: Осін О. Д.
Прийняв: Бурлаков В. М.

ДОДАТОК В

Діаграма архітектури системи

Діаграма архітектури системи



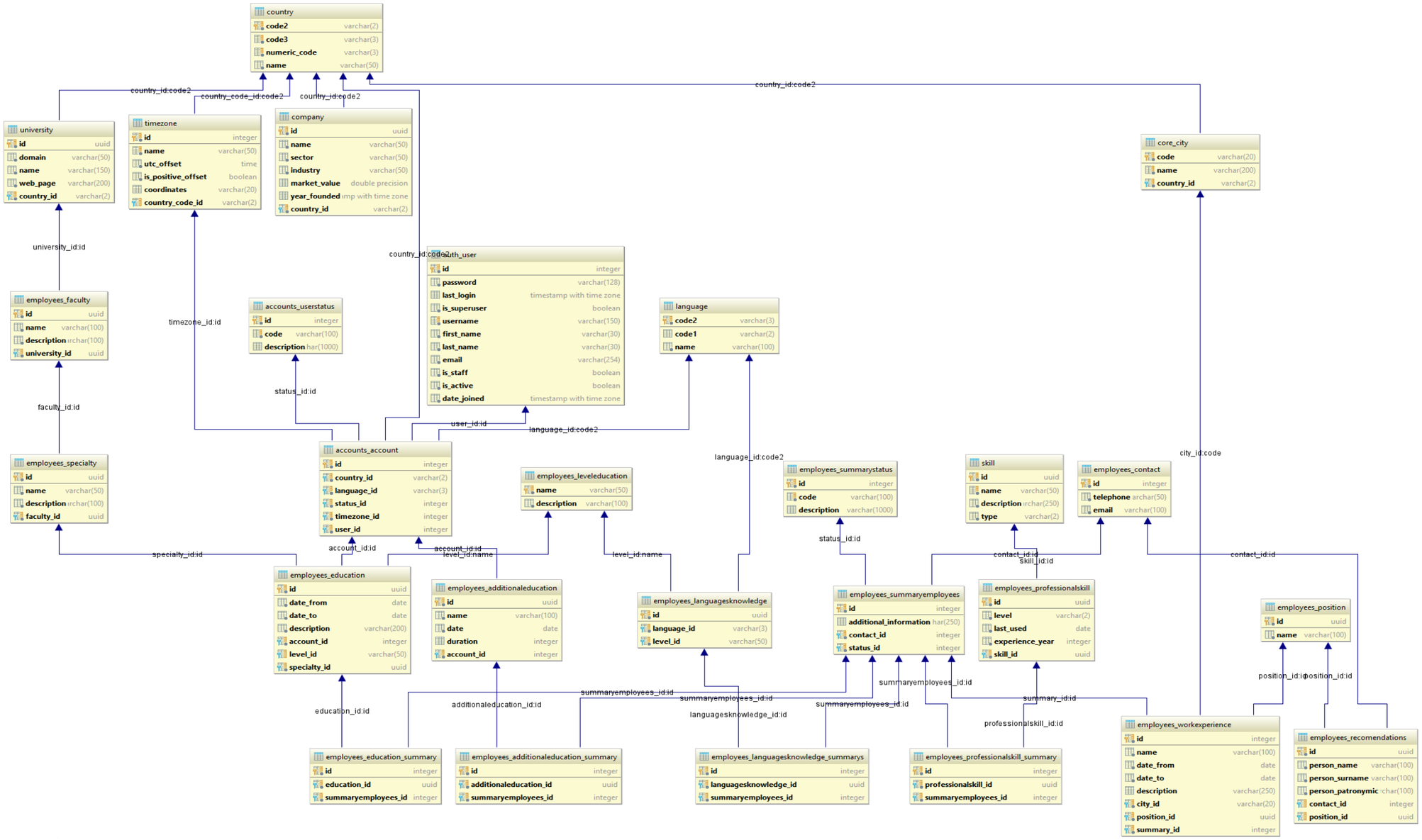
Демонстраційний плакат № 3
до магістерської дисертації на тему
„Система сертифікації даних на основі блокчейн технології”

Розробив: Осін О. Д.
Прийняв: Бурлаков В. М.

ДОДАТОК Г

Діаграма бази даних модуля користувача

Діаграма бази даних модуля користувача



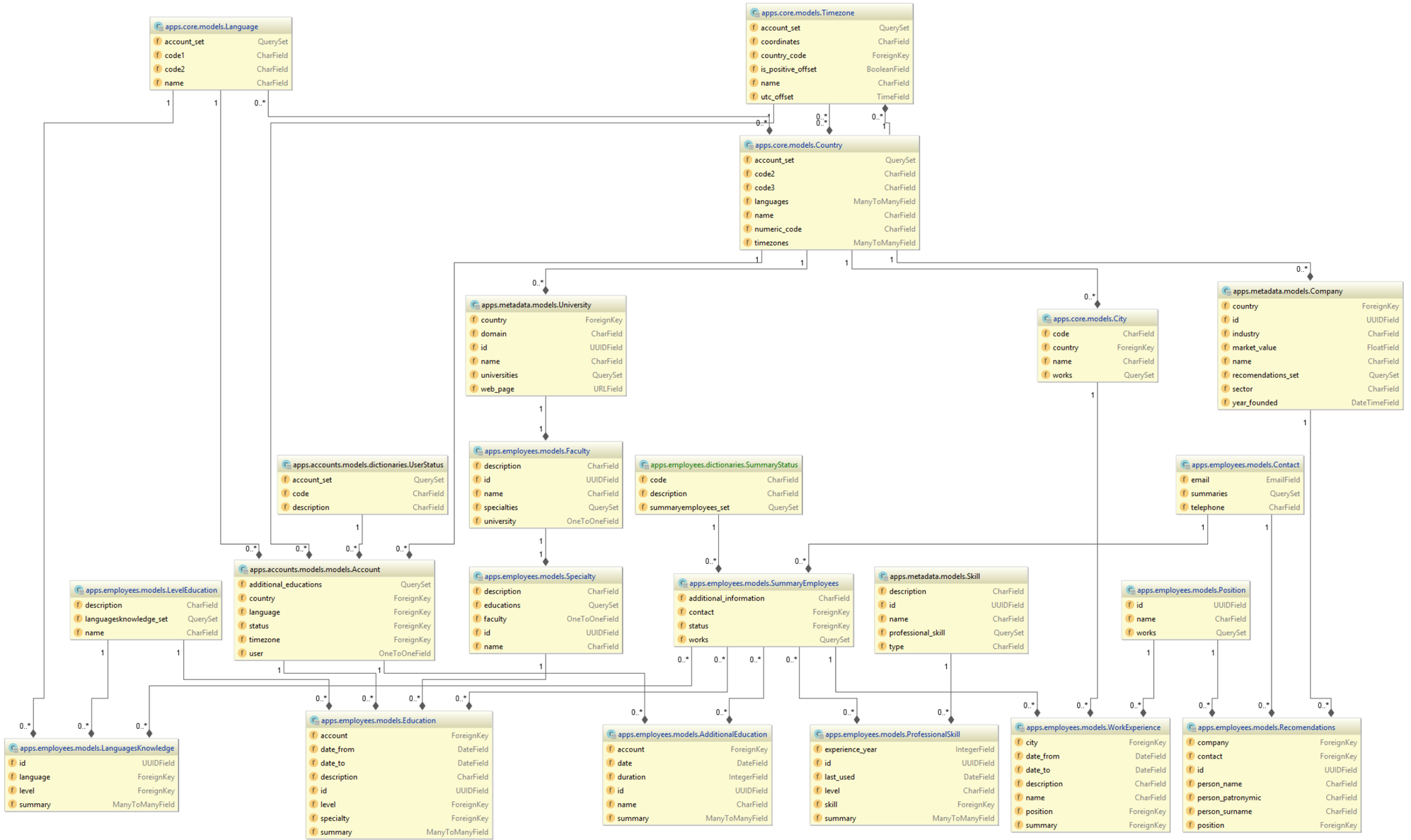
Демонстраційний плакат № 4
до магістерської дисертації на тему
„Система сертифікації даних на основі блокчейн технології”

Розробив: Осін О. Д.
Прийняв: Бурлаков В. М.

ДОДАТОК Д

Діаграма класів модуля користувача

Діаграма класів модуля користувача



Демонстраційний плакат № 5
до магістерської дисертації на тему
„Система сертифікації даних на основі блокчейн технології”

Розробив: Осін О. Д.
Прийняв: Бурлаков В. М.